ОКС 35.040

Изменение № 1 O‘z DSt 1204:2009 **Информационная технология. Криптографическая защита информации. Требования безопасности к криптографическим модулям**

Утверждено и введено в действие постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 13.01.2014 № 05-515

Дата введения 14.01.2014

Срок действия государственного стандарта продлить до 20.03.2019 г.

Раздел 2

В обозначении государственного стандарта O'z DSt 1092 год утверждения «2005» заменить на «2009».

В обозначении государственного стандарта O'z DSt 1105 год утверждения «2006» заменить на «2009».

В обозначении государственного стандарта O'z DSt 1109 год утверждения «2006» заменить на «2013».

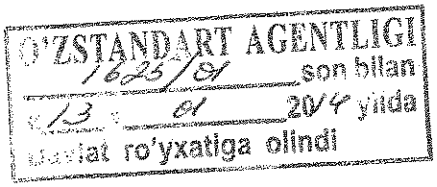
Пункт 3.1

Первое предложение изложить в новой редакции:

«В настоящем стандарте применены термины по O'z DSt 1109, а также следующие термины с соответствующими определениями:»

Библиография

Исключить.



Изменение № 1 O‘z DSt 1204:2009

Вр.и.о. директора
ГУП «UNICON.UZ» _____ Х. Хасанов

Начальник
научно-исследовательского
отдела криптографии _____ О. Ахмедова

Младший научный сотрудник
научно-исследовательского
отдела криптографии _____ Д. Джаматова

Нормоконтроль _____ Л. Шаймарданова
06.12.2013

СОГЛАСОВАНО

Начальник отдела
информационной безопасности
Государственного комитета связи,
информатизации и информационных
технологий Республики Узбекистан

А. Гафуров
письмо от 09.12.2013г.
№ 14-8/6023

O'ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

O‘z DSt 1204 :2009

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Требования безопасности к криптографическим модулям

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Центром научно-технических и маркетинговых исследований (ЦНТМИ) Узбекского агентства связи и информатизации

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 27.02.09 № 05-138

3 ВВЕДЕН ВПЕРВЫЕ

4 В настоящем стандарте реализованы нормы законов Республики Узбекистан «Об электронной цифровой подписи», «Об электронном документообороте» и «Об электронной коммерции»

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
3.1 Термины и определения. 2
3.2 Сокращения. 11
4 Общие положения. 11
5 Уровни безопасности криптографических модулей 12
5.1 Первый уровень безопасности 12
5.2 Второй уровень безопасности 13
5.3 Третий уровень безопасности 14
5.4 Четвертый уровень безопасности. 15
5.5 Пятый уровень безопасности. 17
6 Цели функциональной безопасности 17
7 Требования безопасности 18
7.1 Спецификация криптографического модуля 19
7.1.1 Типы криптографических модулей 20
7.1.2 Криптографическая граница 20
7.1.3 Режимы работы 21
7.1.4 Ограниченные функциональные возможности 21
7.1.5 Стойкость безопасности модуля 22
7.2 Физические порты и логические интерфейсы 22
7.3 Роли, аутентификация и сервисы 24
7.3.1 Роли 24
7.3.2 Аутентификация оператора 25
7.3.3 Сервисы 27
7.4 Безопасность программного обеспечения 28
7.5 Операционная среда 31
7.5.1 Требования к операционной системе для модифицированных операционных сред 32
7.6 Физическая безопасность 36
7.6.1 Общие требования по физической безопасности 37
7.6.2 Защита от воздействий окружающей среды/Тестирование 39
7.6.2.1 Особенности безопасности окружающей среды 40
7.6.2.2 Процедура тестирования на воздействия окружающей среды 40
7.7 Защита от неразрушающих атак 42
7.8 Управление чувствительными параметрами безопасности 42
7.8.1 Генераторы случайных битовых последовательностей . . . 43

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

7.8.2 Генерация чувствительного параметра безопасности 44
7.8.3 Установка чувствительного параметра безопасности 44
7.8.4 Ввод и вывод чувствительного параметра безопасности . 45
7.8.5 Хранение чувствительного параметра безопасности 46
7.8.6 Обнуление чувствительного параметра безопасности 47
7.9 Самотестирование 48
7.9.1 Предпусковое самотестирование. 49
7.9.2 Условное самотестирование 51
7.10 Гарантия жизненного цикла. 53
7.10.1 Управление конфигурацией 53
7.10.2 Проектирование 54
7.10.3 Модель конечного автомата 55
7.10.4 Разработка 56
7.10.5 Тестирование криптографического модуля поставщиком 57
7.10.6 Доставка и презентация 58
7.10.7 Руководящие документы 58
7.11 Подавление прочих атак 60
Приложение А (обязательное) Краткие требования к документации. 61
Приложение В (обязательное) Политика безопасности криптографического модуля. 67
Библиография 72

O‘z DSt 1204 :2009

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Ахборот технологияси
АХБОРОТНИНГ КРИПТОГРАФИК МУҲОФАЗАСИ
Криптографик модулларга хавфсизлик талаблари

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Требования безопасности к криптографическим модулям

Information technology
CRYPTOGRAPHIC DATA SECURITY
Security Requirements for Cryptographic Modules

Дата введения 20.03.09
20.03.2014

1 Область применения

Настоящий стандарт устанавливает единые требования безопасности к криптографическим модулям с открытым и симметричным ключом и предназначен для применения при проектировании, разработке, производстве, реализации (доставке) и эксплуатации средств криптографической защиты информации. Стандарт определяет требования безопасности к криптографическим модулям, используемым для защиты конфиденциальной информации, хранимой и передаваемой в сетях ЭВМ, телекоммуникаций, в отдельных вычислительных комплексах или в ЭВМ.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O'z DSt 1092:2005 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

O'z DSt 1105:2006 Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных.

O'z DSt 1109:2006 Информационная технология. Криптографическая защита информации. Термины и определения.

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на территории Узбекистана по соответствующему

O'ZSTANDART AGENTLIGI
1625 son bilan
«27» 02 2009 yilda
Davlat ro'yxatiga olindi

указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **аппаратные средства** (hardware): Физическое оборудование в пределах криптографической границы, используемое для обработки программ и данных (включает в себя не перепрограммируемое программное обеспечение).

3.1.2 **аппаратный модуль** (hardware module): Модуль, составленный, прежде всего из аппаратных средств, которые могут также содержать некоторое программное обеспечение.

3.1.3 **аутентификационные данные** (authentication data): Информация, используемая для верификации предъявленного идентификатора пользователя.

3.1.4 **вектор инициализации** (initialization vector): Вектор, используемый для определения отправной точки криптографического процесса в пределах криптографического алгоритма.

3.1.5 **входная информация сервиса** (service input): Все данные или информация управления, используемая криптографическим модулем для инициализации или реализации определенных операций или функций.

3.1.6 **входные данные** (input data): Информация, которая вводится в криптографический модуль в целях преобразования или вычисления по утвержденной в установленном порядке функции безопасности.

3.1.7 **временной анализ** (timing analysis): Атака на криптографический модуль, которая основана на анализе периодов времени между временем запуска команды и временем получения результата.

3.1.8 **выходная информация сервиса** (service output): Все данные и информация об статусе, которые являются результатами выполнения операций или функций, инициализированных или полученных на основе ввода сервиса.

3.1.9 **выходные данные** (output data): Информация, выработанная криптографическим модулем.

3.1.10 **генератор случайных битовых последовательностей** (random bit generator): Устройство или алгоритм, генерирующий последовательность битов, биты которой статистически независимы и не смещены друг от друга.

3.1.11 **гибридный модуль** (hybrid module): Модуль, криптографические функциональные возможности которого прежде всего обеспечиваются программным обеспечением, и который также включает некоторые специализированные аппаратные средства в пределах криптографической границы модуля.

3.1.12 **двухфакторная аутентификация** (two-factor authentication): Тип аутентификации, который требует два независимых метода установления идентификации и авторизации для выполнения сервисов.

3.1.13 **дифференциальный анализ мощности** (differential power analysis): Анализ изменений электрической потребляемой мощности криптографическим модулем с использованием передовых статистических методов и/или других методов, с целью раскрытия информации, коррелированной с криптографическим ключом, используемым в криптографическом алгоритме.

3.1.14 **доверенный канал** (trusted channel): Канал, гарантирующий целостность передаваемой информации с взаимной аутентификацией сторон обмена и обеспечивающий доверенную, безопасную и дискретную связь для обмена чувствительными параметрами безопасности и другой критической информацией между криптографическим модулем и предназначенной оконечной точкой связи модуля.

3.1.15 **доказательство вмешательства** (tamper evidence): Внешняя индикация о совершенной попытке скомпрометировать физическую безопасность криптографического модуля. (Доказательство попытки вмешательства должно быть замечено оператором немедленно.)

3.1.16 **зашифрованный ключ** (encrypted key): Криптографический ключ, который зашифрован с использованием утвержденной в установленном порядке функции безопасности и ключа для шифрования ключа.

3.1.17 **защита от воздействий окружающей среды** (environmental failure protection): Предотвращение компрометации безопасности криптографического модуля с помощью использования защиты от воздействий окружающей среды или колебаний параметров от установленного для данного модуля нормального диапазона значений.

3.1.18 **информация о состоянии** (status information): Информация, которая выводится из криптографического модуля для индикации некоторых операционных свойств или состояний модуля.

3.1.19 **интерфейс** (interface): Логическая входная или выходная точка криптографического модуля, обеспечивающая доступ к модулю для

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

логических потоков информации, представленных в виде физических сигналов.

3.1.20 **интерфейс программного обеспечения модуля** (module software interface): Набор команд, используемый для ввода запроса сервисов модуля, включая вводимые или выводимые из криптографической границы модуля параметры, как части требуемого сервиса.

3.1.21 **ключ для шифрования ключа** (key encrypting key): Криптографический ключ, используемый для зашифрования или расшифрования других ключей.

3.1.22 **код обнаружения ошибок** (error detection code): Код, вычисленный в функции от данных и составленный из избыточных битов информации, предназначенных для обнаружения неумышленной модификации, но не для исправления ошибок.

3.1.23 **код аутентификации сообщений** (message authentication code): Последовательность битов фиксированной длины, вырабатываемая из данных с использованием секретного ключа и добавляемая к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.

3.1.24 **компонента криптографического ключа, ключевая компонента** (cryptographic key component, key component): Параметр, используемый совместно с другими ключевыми компонентами в утвержденных в установленном порядке функциях безопасности для формирования открытого текста криптографического ключа или исполнения криптографической функции.

3.1.25 **критичный параметр безопасности** (critical security parameter): Информация, связанная с безопасностью, которая появляется в открытом тексте либо в другой незащищённой форме, разглашение или модификация которой может скомпрометировать безопасность криптомодуля или безопасность информации, обрабатываемой модулем. Например, секретные криптографические ключи, особые личные ключи, данные, связанные с аутентификацией (пароли, PIN-коды).

3.1.26 **криптосотрудник** (cryptographic officer): Оператор или процесс (субъект), действующий в роли оператора, осуществляющего криптографическую инициализацию или управление функциями.

3.1.27 **криптографическая граница** (cryptographic boundary): Явно определенный непрерывный периметр, который устанавливает физические границы криптографического модуля и содержит все аппаратные и/или программные компоненты криптографического модуля.

3.1.28 **криптографическая функция хэширования** (cryptographic hash function): Эффективно вычисляемая функция, отображающая строки

бит (прообраз) в строки бит (образ) фиксированной длины так, что вычислительно трудно найти два различных прообраза с общим образом.

3.1.29 **криптографически защищенный критичный параметр безопасности** (cryptographically protected critical security parameters): Критичный параметр безопасности, который криптографически защищен от несанкционированного разглашения, модификации и замены, защитные механизмы которого реализовываются только на утвержденных в установленном порядке функциях безопасности.

3.1.30 **криптографически защищенный чувствительный параметр безопасности** (cryptographically protected sensitive security parameters): Либо криптографически защищенный критичный параметр безопасности, либо криптографически защищенный открытый параметр безопасности.

3.1.31 **логическая защита** (logical protection): Защита от несанкционированного доступа (включая несанкционированное использование, модификацию, замену и, в случае критичного параметра безопасности, раскрытие) посредством интерфейса программного обеспечения модуля под управлением операционной системы. Логическая защита программного обеспечения не обеспечивает защиту чувствительного параметра безопасности от физического вмешательства.

3.1.32 **личный ключ** (private key): Криптографический ключ, однозначно связанный с субъектом и не являющийся открытым, используемый в криптографическом алгоритме с открытым ключом.

3.1.33 **модель конечного автомата** (finite state model): Математическая модель последовательной машины, которая состоит из конечного множества входных событий, конечного множества событий выхода, конечного множества состояний; функции, отображающей состояния с входом в выход; функции, отображающей состояния и входы в состояния (функция перехода состояний) и спецификации, описывающей начальное состояние.

3.1.34 **маршрут данных** (data path): Физический или логический маршрут, по которому проходят данные (физический маршрут данных может быть разветвлен многими логическими путями данных).

3.1.35 **механизмы аутентификации** (authentication mechanisms): Пароли, персональные карточки или иные устройства аналогичного назначения, криптографические методы, устройства измерения и анализа биометрической информации, используемые для аутентификации.

3.1.36 **микропрограмма** (microcode): Элементарные команды процессора, которые соответствуют выполнимой команде программы.

3.1.37 **модифицируемая операционная среда** (modifiable operational environment): Операционная среда, которая разработана с использованием какого-либо неутвержденного программного обеспечения.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

3.1.38 **начальный ключ** (seed key): Секретное значение, используемое для инициализации криптографической функции или операции.

3.1.39 **неразрушающая атака** (non-invasive attack): Атака на криптографический модуль без непосредственного физического контакта с ним.

3.1.40 **немодифицируемая операционная среда** (non-modifiable operational environment): Операционная среда, которая разработана только на базе утвержденного в установленном порядке программного обеспечения.

3.1.41 **непрозрачность** (opaque): Непроницаемость световых волн в пределах видимого спектра в диапазоне 400-750 nm; прозрачный либо полупрозрачный в пределах видимого спектра.

3.1.42 **объект** (object): Логический объект, доступ к которому контролируется (например, человек, группа людей, устройство или процесс).

3.1.43 **обнаружение вмешательства** (tamper detection): Автоматическое определение криптографическим модулем, что совершена попытка скомпрометировать его физическую безопасность.

3.1.44 **обнуление** (zeroization): Метод стирания хранимых в электронном виде данных, исключающий возможность их восстановления.

3.1.45 **операционная среда** (operational environment): Совокупность программного обеспечения и оборудования, необходимого для обеспечения надежного функционирования модуля.

3.1.46 **оператор** (operator): Субъект, имеющий доступ к криптографическому модулю или процессу (субъекту), работающий от имени пользователя, независимо от принятой роли.

3.1.47 **особый аппаратный модуль** (specific hardware module): Модуль, состоящий, в основном, из аппаратной части с секретным блоком с встроенным особым личным ключом уполномоченного субъекта.

3.1.48 **особый личный ключ** (specific private key): Криптографический ключ, однозначно связанный с уполномоченным субъектом и не являющийся открытым, используемый в асимметричных и симметричных криптографических алгоритмах (например, тройка параметров R, g, κ_h, где: R – параметр степени, g – основание, κ_h – ключ хэширования).

3.1.49 **отказ от сервиса** (bypass capability): Отказ от оказания сервиса шифрованию или криптографической аутентификации.

3.1.50 **открытый ключ** (public key): Криптографический ключ, являющийся открытым и однозначно связанный с субъектом, который используется в криптографическом алгоритме с открытым ключом (открытые ключи не являются критическими параметрами безопасности).

3.1.51 **открытый параметр безопасности** (public security parameter): Относящаяся к безопасности информация, модификация которой может скомпрометировать безопасность криптографического модуля.

3.1.52 **персональный идентификационный номер (PIN–код)** (personal identification number, PIN): Цифровой код или пароль, используемый для аутентификации субъекта.

3.1.53 **порт** (port): 1. Точка физического входа или выхода в криптографический модуль, которая обеспечивает доступ к модулю физических сигналов, представленных логическими информационными потоками (физически отделенные порты не являются частью одного и того же физического штекера или проволоки). 2. Точка подключения внешнего устройства к внутренней шине микропроцессора; программа может посылать данные в порты или получать их из портов.

3.1.54 **предпусковое тестирование** (pre-operational test): Испытание, выполняемое над криптографическим модулем в промежутке времени от момента включения до момента времени, когда криптографический модуль начнет использовать функцию или предоставлять сервисы с использованием тестируемой функции.

3.1.55 **промышленный уровень** (production grade): Промышленное стандартное производство.

3.1.56 **политика безопасности криптографического модуля** (cryptographic module security policy): Описание того, насколько конкретный модуль должен удовлетворять требованиям безопасности данного стандарта и дополнительным критериям поставщика (торгового органа).

3.1.57 **программное обеспечение** (software): Программы внутри криптографической границы, обычно сохраняемые на стираемых носителях (например, на дисках), и которые могут быть динамически записаны, изменены или перепрограммированы.

3.1.58 **программный модуль** (software module): Модуль, который состоит исключительно из программного обеспечения.

3.1.59 **пользователь** (user): Личность или процесс, действующий от имени субъекта, который обращается к криптографическому модулю за получением криптографических сервисов.

3.1.60 **радиационная закалка** (radiation hardening): Повышение способности устройства или части оборудования противостоять против ядерной или другой радиации; применяется в основном по отношению к диэлектрикам и полупроводниковым материалам.

3.1.61 **руководство к выполнению** (implementation guidance): Набор документов, изданных в течение жизненного цикла стандарта, который содержит дополнительные разъяснения, руководство по тестированию и интерпретации стандарта (Руководство к выполнению не может содержать отличающиеся от стандарта требования).

3.1.62 **ручной ввод ключа (чувствительного параметра безопасности)** (manual key (sensitive security parameter) entry): Ввод

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

криптографических ключей в криптографический модуль с помощью клавиатуры.

3.1.63 **реакция на вмешательство** (tamper response): Автоматическое действие, предпринимаемое криптографическим модулем, когда обнаружено вмешательство.

3.1.64 **рекомендованный** (validated): Рекомендованный уполномоченным органом.

3.1.65 **разделение знания** (split knowledge): Процедура разделения криптографического ключа на несколько ключевых компонент, каждая из которых не содержит никакого знания об оригинальном ключе и которая может быть впоследствии введена в криптографический модуль или выведена из него отдельными субъектами и объединена с другими компонентами в целях обновления оригинального криптографического ключа.

3.1.66 **системное программное обеспечение** (system software): Специальное программное обеспечение в пределах криптографической границы модуля (например, операционная система, компилятор или утилита), предназначенное для облегчения работы и обслуживания специализированной компьютерной системы или семейства компьютерных систем, компьютерной системы, а также взаимосвязанных с ними программ и данных.

3.1.67 **сервис** (service): Любая внешне вызванная операция или/и функция, которая может быть выполнена криптографическим модулем.

3.1.68 **система управления конфигурацией** (configuration management system): Управление видами и гарантией безопасности посредством управления производимыми изменениями в аппаратном и программном обеспечениях, а также в документации криптографического модуля.

3.1.69 **согласование ключей** (key agreement): Процесс, используемый двумя или несколькими сторонами, чтобы согласовать секретный симметричный ключ.

3.1.70 **стойкость безопасности** (security strength): Число, связанное с объемом работ (то есть количеством операций), которое требуется для взлома криптографического алгоритма или модуля.

3.1.71 **субъект** (subject): Активный логический объект, имеющий доступ к объектам.

3.1.72 **съемная крышка** (removable cover): Часть корпуса криптографического модуля, позволяющая осуществить физический доступ к содержимому модуля.

3.1.73 **тестирование на воздействия окружающей среды** (environmental failure testing): Использование определенных испытательных

методов для обеспечения разумной гарантии, чтобы не допускать компрометации безопасности криптографического модуля из-за воздействий окружающей среды или колебаний параметров от установленных для данного модуля нормального диапазона значений.

3.1.74 **транспортировка ключа** (key transport): Безопасная транспортировка криптографических ключей (критичных параметров безопасности) от одного криптографического субъекта к другому субъекту.

3.1.75 **управление ключом** (key management): Действия, выполняемые в течение всего жизненного цикла ключей, включая управление криптографическими ключами и другими параметрами, связанными с безопасностью (например, векторами инициализации и паролями), а также их генерацию, хранение, установку, ввод, вывод и обнуление.

3.1.76 **упрощенный анализ мощности** (simple power analysis): Непосредственный (первоначальный визуальный) анализ исполнения набора инструкций (или исполнения отдельных инструкций), полученного посредством мониторинга изменений потребления электрической мощности криптографическим модулем для обнаружения неполадок и результатов исполнения криптографических алгоритмов при различных значениях криптографических ключей.

3.1.77 **уполномоченный орган** (validation authority): Орган, осуществляющий единую государственную политику и обеспечивающий проведению сертификации продукции (услуг) в области криптографической защиты информации.

3.1.78 **уполномоченный субъект** (validation subject): Лицо, которое является уполномоченным со стороны организации, занимающейся проектированием модуля, или со стороны центра регистрации ключей.

3.1.79 **утвержденный метод аутентификации данных** (approved data authentication technique): Утвержденный в установленном порядке метод, который может включать использование электронной цифровой подписи и кода аутентификации сообщения на основе ключевых хэш-функций.

3.1.80 **утвержденный режим работы** (approved mode of operation): Режим криптографического модуля, который использует только те функции безопасности, которые утверждены в установленном порядке или санкционированы уполномоченным органом.

3.1.81 **утвержденная функция безопасности** (approved security function): Функция безопасности (т.е., криптографический алгоритм, который может быть протестирован, или метод аутентификации), которая входит в перечень функций безопасности, утвержденных уполномоченным органом в установленном порядке.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

3.1.82 **управляющая информация** (control information): Информа-ция, которая вводится в криптографический модуль с целью управления операциями модуля.

3.1.83 **установка (инициализация) ключа** (key establishment): Процесс безопасного установления криптографических ключей в криптографических модулях с использованием транспортировки и/или процедур согласования ключей.

3.1.84 **условный тест** (conditional test): Тест, выполняемый над криптографическим модулем при определенных условиях.

3.1.85 **физическая защита** (physical protection): Защита криптографического модуля, криптографических ключей или критичных параметров безопасности с помощью физических средств.

3.1.86 **чувствительные данные** (sensitive data): Данные, которые с точки зрения пользователя нуждаются в защите.

3.1.87 **чувствительные параметры безопасности** (sensitive security parameters): Критичные и открытые параметры безопасности.

3.1.88 **целостность** (integrity): Устойчивость чувствительных данных к модификации или удалению несанкционированным способом без обнаружения.

3.1.89 **энтропия минимума** (min-entropy): Самая худшая мера (то есть самая верхняя среди нижних границ) неопределенности для случайной переменной.

3.1.90 **электромагнитные излучения** (electromagnetic emanations): Сигналы, несущие в себе сведения, захват и анализ которых обеспечивают потенциальную возможность раскрытия конфиденциальной информации (переданной полученной, обработанной или иначе обработанной любым устройством обработки данных).

3.1.91 **электронный ввод ключа** (electronic key entry): Ввод криптографических ключей в криптографический модуль с использованием электронных методов, например, смарт-карт или загружающего устройства. (Оператор, вводящий ключ не может иметь никаких сведений о значении вводимого ключа.)

3.1.92 **электронная транспортировка (передача) ключа** (electronic key transport): Транспортировка криптографических ключей, обычно в зашифрованной форме, с использованием электронных средств, например, компьютерной сети, на основе протоколов распределения/согласования ключа.

3.1.93 **электростатический разряд** (electrostatic discharge): Внезапный и мгновенный электрический ток, который течет, когда избыток электрического заряда, сохраненного на электрически изолированном

объекте, находит путь к другому объекту (например, корпусу или заземлению), имеющему другой электрический потенциал.

3.1.94 **энтропия** (entropy): Мера неопределенности источника сообщений, определяемая вероятностями появления тех или иных символов при их передаче.

3.2 Сокращения

В настоящем стандарте используются следующие сокращения:

ВА (TA)	временной анализ (Timing analyses)
ГСБП (RBG)	генератор случайных битовых последовательностей (Random Bit Generator)
ДАМ (DPA)	дифференциальный анализ мощности (Differential Power Analysis)
ИПМ (MSI)	интерфейс программного модуля (Module Software Interface)
КПБ (CSP)	критичный параметр безопасности (Critical Security Parameter)
КМ (KM)	криптографический модуль (Cryptographic Module)
КАС (MAC)	код аутентификации сообщений (Message Authentication Code)
КС (CO)	криптосотрудник (Cryptographic Officer)
КОО (EDC)	код обнаружения ошибок (Error Detection Code)
МКА (FSM)	модель конечного автомата (Finite State Model)
ОПБ (PSP)	открытый параметр безопасности (Public Security Parameters)
ОС (OS)	операционная система (Operational System)
ПО (SW)	программное обеспечение (Software)
СУК (CMS)	система управления конфигурацией (Configuration Management System)
УАМ (SPA)	упрощенный анализ мощности (Simple Power Analysis)
ЧПБ (SSP)	чувствительный параметр безопасности (Sensitive Security Parameter)
ЭМИ (EME)	электромагнитные излучения (Electromagnetic Emanation)
ЭЦП (EDS)	электронная цифровая подпись (Electronic Digital Signature)
ЯОАО (HDL)	язык описания аппаратного обеспечения (Hardware Description Language)

4 Общие положения

Настоящий стандарт устанавливает в возрастающем порядке пять квалификационных уровней безопасности в одиннадцати потенциально

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

возможных сферах применения и окружения криптографических модулей. К этим сферам относятся: спецификация криптографического модуля; физические порты и логические интерфейсы криптографического модуля; роли, аутентификация и сервисы; безопасность программного обеспечения; операционная среда; физическая безопасность; физическая защита от неразрушающих атак; управление чувствительными параметрами; самотестирование; гарантия жизненного цикла криптографического модуля; подавление других атак.

Требования безопасности, выполнение которых должно быть гарантировано конкретным криптографическим модулем, устанавливаются одним из пяти уровней безопасности: первый уровень самый низкий, а пятый - самый высокий уровень требований безопасности.

Уровень безопасности зависит от информационного риска, т.е. фактора, отображающего возможный ущерб в результате реализации предполагаемого набора угроз информационной безопасности. В конечном итоге риск может отображать достоверные финансовые потери. Чем выше уровень возможного ущерба, тем выше должен быть уровень безопасности криптографического модуля, и это должно определяться соответствующими нормативными документами для конкретного ведомства, организации или предприятия по итогам анализа рисков и уязвимостей системы безопасности.

Примечание – В Республике Узбекистан запрещается применение стандартов зарубежных стран (например, стандарты США (DES, DSA) и Российской Федерации (ГОСТ Р 34.10-94)), стойкость, которых ниже чем стойкость национальных стандартов.

5 Уровни безопасности криптографических модулей

5.1 Первый уровень безопасности

Первый уровень безопасности соответствует криптографическим модулям без защитных механизмов. Криптографический модуль на данном уровне безопасности создан по крайней мере на базе одной утвержденной в установленном порядке функции безопасности; кроме компонентов промышленного уровня никакие другие специальные механизмы безопасности не требуются. Примером может служить плата персонального компьютера, смарт-карта и др.

Первый уровень безопасности позволяет реализовывать программные компоненты криптографического модуля на универсальных компьютерных системах с использованием неоцененных операционных систем. Такое выполнение может соответствовать для безопасных приложений, где управление физической и сетевой безопасностью, а также административные процедуры обеспечиваются вне модуля.

Примечание – Для криптографических модулей, разработанных на базе O'z DSt 1105, при длине входного блока в 128 или 256 bit длина ключа шифрования должна составлять 128 или 256 bit, соответственно.

Для аппаратных, программных и гибридных модулей, разработанных на базе O'z DSt 1092, в режиме с сеансовым ключом модуль p должен удовлетворять условию $2^{576} \le p < 2^{640}$, а параметр R должен являться открытым только относительно группы санкционированных пользователей, в режиме без сеансового ключа модуль p должен удовлетворять условию $2^{1024} \le p < 2^{2048}$.

Для особых аппаратных модулей, разработанных на базе O'z DSt 1092, модуль p должен удовлетворять условию $2^{256} \le p < 2^{384}$.

5.2 Второй уровень безопасности

Второй уровень безопасности относится к криптографическим модулям *с обнаружением взломов.* Данный уровень безопасности криптографического модуля расширяет физические механизмы безопасности первого уровня, добавляя требование доказательства вмешательств. На криптографическом модуле имеются покрытия и (или) печати на ударопрочных замках съемных крышек или дверцах, предназначенные для обнаружения факта вскрытия или попытки вскрытия. Покрытия и (или) печати выполняются таким образом, чтобы они разрушались при физическом доступе к КПБ модуля. Они расположены на крышках или дверцах для защиты от несанкционированного физического доступа.

Второй уровень безопасности требует аутентификации на основе роли, согласно которой криптографический модуль подтверждает подлинность разрешения оператора принять определенную роль и исполнить соответствующий набор сервисов.

Второй уровень безопасности позволяет выполнить программные компоненты криптографического модуля на универсальной вычислительной системе с использованием операционной системы, которая:

a) обеспечивает контролируемое управление доступом, которое защищает от несанкционированного использования, модификации и чтения криптографического программного обеспечения, и

b) обеспечивает контрольные механизмы для регистрации модификаций, доступов, удалений и добавлений криптографических данных и чувствительных параметров безопасности.

Операционная система, осуществляющая этот контроль, обеспечивает такой уровень доверия (логическую защиту), при котором криптографические модули, выполняющиеся на универсальных вычислительных платформах, были бы сопоставимы с криптографическими модулями, построенными с использованием специализированных аппаратных систем.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Примечание – Для криптографических модулей, разработанных на базе O’z DSt 1105, длина входного блока и ключа шифрования должна составлять 256 bit.

Для аппаратных, программных и гибридных модулей, разработанных на базе O’z DSt 1092, в режиме с сеансовым ключом модуль p должен удовлетворять условию $2^{640} \le p < 2^{704}$, параметр R должен являться открытым только относительно группы санкционированных пользователей, а параметр R_1 должен являться симметричным ключом для пары санкционированных пользователей, в режиме без сеансового ключа модуль p должен удовлетворять условию $2^{1024} \le p < 2^{2048}$.

Для особых аппаратных модулей, разработанных на базе O’z DSt 1092, модуль p должен удовлетворять условию $2^{384} \le p < 2^{512}$.

5.3 Третий уровень безопасности

Третий уровень безопасности относится к криптографическим модулям с *предотвращением взлома.* В дополнение к физическим механизмам безопасности по обнаружению вмешательств, требуемым на втором уровне, третий уровень безопасности предотвращает несанкционированный доступ к КПБ в пределах криптографического модуля.

Физические механизмы безопасности, требуемые на данном уровне безопасности, предназначены для обеспечения высокой вероятности обнаружения и принятия ответной меры к попыткам прямого физического доступа и несанкционированного использования или модификации криптографического модуля. Эти механизмы могут включать использование прочных корпусов, средства обнаружения вмешательства и схему реагирования посредством обнуления всего открытого текста КПБ при вскрытии съемных крышек или дверцы криптографического модуля.

Третий уровень безопасности требует наличия механизмов распознавания на основе аутентификации и идентификации, расширяя механизмы аутентификации на основе роли, типичной для второго уровня безопасности. Криптографический модуль подтверждает подлинность аутентификации оператора и проверяет, уполномочен ли аутентифицированный оператор принять предназначенную ему роль и исполнить соответствующий набор сервисов.

Третий уровень безопасности требует, чтобы ввод или вывод КПБ (включая ввод или вывод КПБ с использованием процедур разделения знания частей секрета) был выполнен с использованием портов приёма-передачи данных, физически разделенных друг от друга, или логически разделенных интерфейсов от других интерфейсов, с помощью доверенного канала. КПБ может быть либо введен в модуль, либо выведен из криптографического модуля в зашифрованной форме или с использованием процедуры разделения знания частей секрета.

Третий уровень безопасности требует введения механизмов для защиты КПБ от атак временного анализа.

Третий уровень безопасности допускает выполнение программных компонентов криптографического модуля на универсальной вычислительной системе общего назначения, с использованием операционной системы, которая:

a) препятствует операторам-пользователям модифицировать криптографическое программное обеспечение модуля, системные чувствительные параметры безопасности и контрольные данные, хранимые в операционной среде модуля;

b) осуществляет передачу всех ЧПБ, аутентификационных данных, управляющих введенных и выведенных данных о состоянии через доверенный канал, и

c) осуществляет аудит функционирования доверенного канала.

Создание доверенного канала защищает исходный текст КПБ и программное обеспечение криптографического модуля от не заслуживающих доверия программ, которые могут выполняться в системе или могут быть имитированы удаленными системами.

Третий уровень безопасности требует дополнительных гарантий жизненного цикла, например, автоматизированного управления конфигурацией, детального проектирования, испытания нижнего уровня и аутентификации оператора с использованием аутентификационной информации, обеспеченной поставщиком.

Примечание – Для криптографических модулей, разработанных на базе O'z DSt 1105, длина входного блока должна составлять 256 bit и длина ключа шифрования должна составлять 256 или 512 bit.

Для аппаратных, программных и гибридных модулей, разработанных на базе O'z DSt 1092, в режиме с сеансовым ключом модуль p должен удовлетворять условию $2^{704} \le p < 2^{768}$, параметр R должен являться открытым только относительно группы санкционированных пользователей, а параметр R_1 должен являться симметричным ключом для пары санкционированных пользователей, в режиме без сеансового ключа модуль p должен удовлетворять условию $2^{1024} \le p < 2^{2048}$.

Для особых аппаратных модулей, разработанных на базе O'z DSt 1092, модуль p должен удовлетворять условию $2^{512} \le p < 2^{640}$.

5.4 Четвертый уровень безопасности

Четвертый уровень безопасности относится к криптографическим модулям с *уничтожением данных при взломе.* На данном уровне физические механизмы безопасности обеспечивают весь набор мер безопасности вокруг криптографического модуля с целью обнаружения и принятия ответных мер ко всем несанкционированным попыткам физического доступа. Проникновение в корпус криптографического модуля по любому направлению имеет высокую вероятность обнаруживаемости, и приводит к немедленному обнулению всего открытого текста КПБ. Настоящий уровень

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

безопасности криптографических модулей полезен для работы в физически незащищенных средах.

На четвертом уровне безопасности предусматриваются требования двухфакторной аутентификации во время аутентификации оператора. При этом требуются два из следующих трёх атрибутов:

a) кое-что известное (секретный пароль);

b) кое-что имеющееся (физическая клавиша, маркер, устройство или ключ);

c) физическое свойство (биометрические данные).

Четвертый уровень безопасности также защищает криптографический модуль против компрометации безопасности из-за экологических условий или колебаний напряжения и температуры от нормального диапазона значений, определенных для данного модуля. В криптографическом модуле необходимо либо использовать специальные виды защиты окружающей среды, предназначенные для обнаружения колебаний и обнуления КПБ, либо подвергнуть модуль строгому экологическому испытанию от отклонений с целью обеспечения разумной гарантии того, что модуль не будет поражен колебаниями от установленного для модуля нормального диапазона способом, которым может быть скомпрометирована безопасность модуля.

Модули четвертого уровня требуют защиты КПБ от упрощенного анализа мощности и атак дифференциального анализа мощности. Модуль четвертого уровня должен содержать программное обеспечение, предназначенное для шифрования и аутентификации КПБ, а также для тестирования кода целостности, когда модуль находится в нерабочем состоянии. Это обеспечит надежную защиту КПБ от неавторизированного вскрытия и модификации во время модуля в не рабочем состоянии.

Модули четвертого уровня допускают выполнение программных компонент криптографического модуля на универсальной вычислительной системе с использованием операционной системы, обеспечивающей ревизию всех доступов оператора к данным аудита, всех запросов для использования аутентификационных механизмов организации данных, относящихся к безопасности всех используемых функций криптосотрудником, а также всех запросов к аутентификационным данным, связанным с криптографическим модулем.

Примечание – Для криптографических модулей, разработанных на базе O’z DSt 1105, длина входного блока должна составлять 256 bit и длина ключа шифрования должна составлять 256 или 512 bit.

Для аппаратных, программных и гибридных модулей, разработанных на базе O’z DSt 1092 , в режиме с сеансовым ключом модуль p должен удовлетворять условию $2^{768} \le p < 2^{1024}$, параметр R должен являться открытым только относительно группы санкционированных пользователей, а параметр R_1 должен являться симметричным

ключом для пары санкционированных пользователей, в режиме без сеансового ключа модуль p должен удовлетворять условию $2^{1024} \le p < 2^{2048}$.

Для особых аппаратных модулей, разработанных на базе O'z DSt 1092, модуль p должен удовлетворять условию $2^{640} \le p < 2^{768}$.

5.5 Пятый уровень безопасности

Пятый уровень безопасности обеспечивает самую высокую степень безопасности. Этот уровень включает все соответствующие виды безопасности более низких уровней, дополнительно к расширенным функциям безопасности. Модуль пятого уровня должен содержать программное обеспечение, предназначенное для шифрования, аутентификации ЧПБ и тестирования кода целостности, которое выполняется, когда модуль находится в нерабочем состоянии. Это обеспечивает надежную защиту во время нахождения модуля в нерабочем состоянии, обнаруживая и предотвращая вскрытие и модификацию как ОПБ, так и КПБ.

Модули пятого уровня имеют механизмы безопасности от изменения условий окружающей среды, защищающих модуль от колебаний температуры и напряжения питания. На данном уровне модуль должен быть непрозрачным к невидимому лучевому сканированию, а схема обнуления должна быть защищена в достаточной мере для выполнения немедленного обнуления ОПБ и КПБ.

На пятом уровне КПБ должен быть защищен от атак на основе электромагнитных излучений.

На пятом уровне проект модулей верифицируется строгим формальным и неформальным доказательством соответствия формальной модели к функциональной спецификации.

Примечание – Для криптографических модулей, разработанных на базе O'z DSt 1105, длина входного блока должна составлять 256 bit и длина ключа шифрования должна составлять 512 bit.

Для аппаратных, программных и гибридных модулей, разработанных на базе O'z DSt 1092 должен быть использован режим с сеансовым ключом и модуль p должен удовлетворять условию $2^{1024} \le p < 2^{4096}$, параметр R_1 должен являться симметричным ключом для пары санкционированных пользователей .

Для особых аппаратных модулей, разработанных на базе O'z DSt 1092, модуль p должен удовлетворять условию $2^{768} \le p < 2^{1024}$.

6 Цели функциональной безопасности

Требования безопасности, установленные в этом стандарте, касаются безопасного проектирования, изготовления и использования криптографического модуля. Требования для криптографического модуля

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

формулируются на основе следующих целей функциональной безопасности высокого уровня:

a) использовать и правильно осуществлять утвержденные в установленном порядке функции безопасности для защиты чувствительной информации;

b) защищать криптографический модуль от несанкционированной операции или использования;

c) предотвратить несанкционированное раскрытие содержимого криптографического модуля;

d) предотвратить несанкционированную и не обнаруживаемую модификацию криптографического модуля и криптографических алгоритмов, включая неавторизированную модификацию, замену, вставку и удаление ЧПБ;

e) обеспечить индикацию рабочего состояния криптографического модуля;

f) гарантировать, что криптографический модуль во время своего функционирования исполняет должным образом все функции в утвержденном в установленном порядке режиме работы модуля;

g) обнаружить ошибки в операциях криптографического модуля и предотвратить компрометацию или модификацию чувствительных данных и ЧПБ вследствие этих ошибок;

h) гарантировать качественное проектирование, распределение и исполнение криптографического модуля;

i) гарантировать безопасное выполнение процедуры встраивания особого личного ключа в аппаратный модуль на стадии разработки или регистрации открытых ключей;

j) гарантировать, что особый аппаратный модуль при всякой попытке извлечения информации об особом личном ключе обеспечивает необратимое обнуление данного ключа.

7 Требования безопасности

Этот раздел определяет требования безопасности, которые должны быть удовлетворены криптографическими модулями, соответствующими этому стандарту. Требования безопасности охватывают области, связанные с проектированием, реализацией (созданием) и функционированием криптографического модуля. Эти области включают криптографическую спецификацию модуля; порты и интерфейсы модуля; роли, аутентификацию и сервисы; программную безопасность; операционную среду; физическую безопасность; защиту от неразрушающих атак; управление чувствительными параметрами безопасности; самотестирование и гарантию жизненного цикла.

Необязательная область, связанная с подавлением прочих атак, в настоящее время не проверена, но поставщик модуля обязан документировать выполненный контроль.

Криптографический модуль должен быть проверен по требованиям каждой области, перечисленной в этом разделе. Криптографический модуль должен быть независимо оценен в каждой области. В дополнение к получению независимых оценок для каждой из областей безопасности, криптографический модуль также должен получить общую оценку. Общая оценка равняется минимальной оценке из независимых оценок, полученных в соответствующих областях.

Каждая область предусматривает возрастающие уровни безопасности с суммирующимися требованиями безопасности для каждого уровня безопасности. Для каждой из этих областей, криптографический модуль получает рейтинг, соответствующий максимальному уровню безопасности, если удовлетворяет всем требованиям соответствующей области.

Поставщик должен обеспечить испытательную лабораторию полным комплектом документации, включая копии руководств пользователя и руководства по инсталляции.

Многие из требований безопасности этого стандарта включают определенные требования к документам в соответствие с приложениями А и В.

7.1 Спецификация криптографического модуля

Криптографический модуль представляет собой совокупность аппаратных средств и программного обеспечения, предназначенных для реализации криптографических функций или процессов, в том числе криптографических алгоритмов, содержащихся в пределах определенной криптографической границы.

Как правило, криптографический модуль используется в утвержденном в установленном порядке режиме работы. В данном режиме должна быть реализована, как минимум, одна утвержденная в установленном порядке функция безопасности.

Все утвержденные в установленном порядке режимы работы должны быть определены в политике безопасности модуля в соответствием с приложением В.

Аппаратные средства и программное обеспечение криптографического модуля могут быть исключены из требований этого стандарта, если поставщик сможет продемонстрировать, что аппаратные средства и программное обеспечение не влияют на безопасность модуля.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHBOSHMASI

Для первого и второго уровня безопасности в политике безопасности криптографического модуля определяются необходимые условия функционирования модуля в утвержденном в установленном порядке режиме работы.

В дополнение к требованиям первого и второго уровней безопасности, для третьего, четвертого и пятого уровней безопасности в политике безопасности криптографического модуля должны быть указаны условия выбора утвержденного в установленном порядке режима работы.

7.1.1 Типы криптографических модулей

В настоящее время существуют криптографические модули следующих типов:

a) *программный модуль* - модуль, который состоит исключительно из программного обеспечения;

b) *гибридный модуль* - модуль, криптографические функциональные возможности которого прежде всего содержатся в программном обеспечении, и который также включает некоторые целенаправленные специальные аппаратные средства в пределах криптографической границы модуля;

c) *аппаратный модуль* - модуль, состоящий прежде всего из аппаратных средств, и который может также содержать некоторое программное обеспечение. Аппаратный модуль включает средства генерации личного ключа владельца и снабжен механизмами защиты от извлечения информации о личном ключе владельца;

d) *особый аппаратный модуль* - модуль, состоящий, в основном, из аппаратной части, которая содержит секретный блок с встроенным особым личным ключом уполномоченного субъекта.

Секретный блок содержит средства генерации личного ключа владельца и снабжен механизмами защиты от извлечения информации об особом личном ключе уполномоченного субъекта и личном ключе владельца. Механизмы защиты содержат процедуры необратимого обнуления при попытках извлечения информации о КПБ, а при выводе данных наложено ограничение на количество генерируемых открытых ключей и на длину результата верификации (в битах).

Аппаратный и особый аппаратный модуль могут использоваться владельцем в двух режимах:

a) режим ввода личного ключа;

b) режим генерации личного ключа самим модулем.

Особый аппаратный модуль становится аппаратным модулем, если особый личный ключ станет известным владельцу модуля.

7.1.2 Криптографическая граница

Криптографическая граница состоит из явно определенного периметра, который устанавливает физическую границу криптографического модуля. Требования данного стандарта должны применяться ко всем компонентам в пределах этой границы, включая все аппаратные средства и программное обеспечение. Криптографическая граница должна включать процессор(ы) и другие аппаратные компоненты, которые составляют операционную среду модуля.

7.1.3 Режимы работы

Криптографический модуль может быть разработан для поддержки набора утвержденных в установленном порядке режимов работы. При исполнении более чем одного утвержденного в установленном порядке режима работы должны быть соблюдены следующие принципы:

a) полный уровень безопасности модуля не будет изменен, если модуль конфигурирован для различных утвержденных в установленном порядке режимов работы;

b) в политике безопасности должен быть описан каждый из утвержденных в установленном порядке режимов работы, реализованный в криптографическом модуле, а также описано, как конфигурирован каждый режим;

c) после реконфигурации одного утвержденного в установленном порядке режима работы до перехода к другому режиму криптографический модуль должен исполнить предпусковые самотестирования (7.9.1);

d) предпусковое самотестирование должно проводиться для всех утвержденных в установленном порядке функций безопасности, используемых в выбранном режиме работы;

e) если реконфигурация от одного утвержденного в установленном порядке режима работы до другого приводит к изменению физического уровня безопасности модуля, оставляя полный уровень безопасности криптографического модуля без изменений, то криптографический модуль должен исполнить обнуление всех КПБ в пределах модуля, за исключением особого секретного ключа.

7.1.4 Ограниченные функциональные возможности

Криптографический модуль может быть разработан для поддержки ограниченных функциональных возможностей (например, модуль может провести самотестирование для одного алгоритма шифрования и поочередно использовать другой алгоритм шифрования) в пределах утвержденного в установленном порядке режима работы. При реализации ограниченных функциональных возможностей криптографического модуля в утвержденном

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

в установленном порядке режиме работы должны соблюдаться следующие принципы:

a) операция с ограниченными функциональными возможностями вводится только при отрицательном исходе предпускового самотестирования;

b) когда криптографический модуль работает с ограниченными функциональными возможностями, то для каждой операционной функции безопасности должны быть сохранены все результаты проведенного самотестирования;

c) не используемые функции безопасности криптографического модуля должны быть отделены от остальных функций безопасности;

d) модуль должен оставаться в режиме с ограниченными функциональными возможностями до успешного завершения процесса тестирования.

7.1.5 Стойкость безопасности модуля

Для каждого модуля следует определить стойкость безопасности. Стойкость безопасности модуля должна соответствовать одной из рекомендуемых стойкостей безопасности и должна быть не менее, чем стойкость безопасности утвержденных в установленном порядке и разрешенных функций безопасности и КПБ в утвержденном в установленном порядке режиме работы.

7.2 Физические порты и логические интерфейсы

Криптографический модуль должен ограничить весь информационный поток и точки физического доступа к физическим портам и логическим интерфейсам, определяющим все точки ввода и вывода модуля. Интерфейсы криптографического модуля должны логически отличаться друг от друга, хотя они могут совместно использовать единый физический порт (например, входные данные и выходные данные могут быть выведены через один и тот же порт) или могут быть распределены через один или более физических портов (например, входные данные могут вводиться как через последовательный, так и через параллельный порт).

Криптографический модуль может использовать несколько независимых каналов телекоммуникаций. Вывод данных для каждого канала телекоммуникаций должен быть заблокирован при выполнении процедур генерации ключа, ручного ввода ключа, самотестирования, загрузки программного обеспечения и обнуления.

Криптографический модуль должен иметь четыре следующих логических интерфейса (они обозначены в дальнейшем как "ввод" и "вывод" модуля):

a) *интерфейс вывода данных.* Все выходные данные (кроме выходных данных состояния через интерфейс вывода состояния и данных, потенциально предназначенных для компрометации особого личного ключа) от криптографического модуля (включая открытый текст, зашифрованный текст, ЧПБ и управляющую информацию для другого модуля) должны выводиться через интерфейс "вывода данных". Для данного канала телекоммуникаций, все выходные данные через интерфейс вывода данных должны быть запрещены, когда имеет место состояние ошибки, до успешного завершения предпускового испытания целостности программного обеспечения (7.9.1);

b) *интерфейс ввода данных.* Все входные данные (кроме данных управления, введенных через интерфейс ввода управления и потенциально способных скомпрометировать особый личный ключ), обрабатываемые криптографическим модулем (включая открытый текст, зашифрованный текст, ЧПБ и информацию о состоянии от другого модуля), должны вводиться через интерфейс ввода данных;

c) *интерфейс ввода управления.* Все входные команды, сигналы и данные управления (включая функциональные запросы, кроме запросов относительно особого личного ключа, в случае использования особого аппаратного модуля и ручных средств манипуляции типа выключателей, кнопок и клавиатуры), используемые для управления функционированием криптографического модуля, должны вводиться через интерфейс ввода управления;

d) *интерфейс вывода состояния.* Все сигналы вывода, кроме сигналов, несущих информацию об особом личном ключе, в случае использования особого аппаратного модуля, индикаторы и данные о состоянии (включая коды возврата и физические индикаторы типа светоизлучающих диодов и дисплеев), используемые для индикации состояния криптографического модуля должны выводиться через интерфейс вывода состояния. Вывод состояния может быть либо неявным, либо явным.

Криптографический модуль должен различать данные управляющей информации для ввода, а также данные информации состояния для вывода.

Электропитание криптографического модуля от внешних источников или аккумуляторов должно подключаться через отдельный разъем. Этот разъем не нужен, если электропитание обеспечивается в пределах криптографической границы криптографического модуля (например, от внутренней батареи или аккумулятора).

Во время ручного ввода ЧПБ, введенные значения могут быть временно отображены для визуальной верификации с целью повышения точности ввода.

Для обеспечения корректного вывода чувствительной информации, необходимо использовать два независимых способа вывода КПБ.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

На первом и втором уровне безопасности ввод и вывод КПБ осуществляется через физические порты и логические интерфейсы, совместно используемые с другими физическими портами и логическими интерфейсами криптографического модуля.

На третьем, четвертом и пятом уровнях безопасности модуль должен использовать отдельно выделенный физический порт для ввода или вывода КПБ или доверенный канал для обеспечения защиты ввода и вывода КПБ в криптографическом модуле. Если используется доверенный канал, то в документации указывается устойчивость безопасности доверенного канала.

7.3 Роли, аутентификация и сервисы

Криптографический модуль должен поддерживать уполномоченные роли для операторов и соответствующие сервисы в пределах каждой роли.

7.3.1 Роли

Криптографический модуль должен поддерживать роль криптосотрудника. Роль криптосотрудника предназначена для выполнения криптографической инициализации или функций управления и общих сервисов безопасности (например, инициализации модуля, управления криптографическими ключами, КПБ и функций аудита).

Криптографический модуль может поддерживать роли пользователя и уполномоченного лица, но не поддерживать роль уполномоченного субъекта с особым личным ключом. Если криптографический модуль поддерживает роль пользователя, то эта роль должна быть принята для исполнения общих сервисов безопасности, включая криптографические операции и другие утвержденные в установленном порядке функции безопасности.

Криптографический модуль может поддерживать и другие роли в дополнение к указанным выше ролям.

Отдельным операторам могут быть назначены различные роли. Если криптографический модуль поддерживает параллельную работу нескольких операторов, то он должен внутри поддерживать разделение ролей, назначенных каждому оператору, и соответствующих сервисов.

Уполномоченные роли применимы ко всем вызываемым сервисам с использованием утвержденных в установленном порядке функций безопасности. Оператор не обязан принять уполномоченную роль для исполнения сервисов, если КПБ не используется, модифицирован, раскрыт или заменен, а ОПБ не использован, изменен или заменен (например, индикация состояния или другие услуги, не затрагивающие безопасность модуля).

В документации должны быть определены все уполномоченные роли, поддерживаемые криптографическим модулем, а также роль уполномоченного субъекта с указанием адреса защищенного помещения и даты встраивания особого личного ключа в особый аппаратный модуль.

7.3.2 Аутентификация оператора

Для подтверждения подлинности оператора, допущенного к модулю и для верификации наличия полномочий оператора исполнять требуемую роль и сервисы, соответствующие данной роли в пределах криптографического модуля могут потребоваться механизмы аутентификации. Со второго по пятый уровни безопасности криптографический модуль должен поддерживать по крайней мере один из следующих механизмов управления доступом к модулю:

a) *аутентификация на основе роли.* Если криптографическим модулем поддерживаются аутентификационные механизмы на основе роли, то оператор и модуль взаимодействуют в следующем порядке: модуль требует, чтобы оператор выбрал одну или несколько ролей неявным либо явным образом; модуль аутентифицирует выбранные роли (или совокупность ролей). От криптографического модуля не требуется аутентифицировать индивидуальную личность оператора. Действия выбора ролей и аутентификации предположения о выбранных ролях могут быть объединены. Если криптографический модуль разрешает оператору изменять роль, то модуль должен аутентифицировать предположение о любой роли, которая предварительно не прошла процедуру аутентификации;

b) *аутентификация на основе идентификации.* Если криптографическим модулем поддерживаются аутентификационные механизмы на основе *идентификации*, то оператор и модуль взаимодействуют в следующем порядке: модуль требует, чтобы оператор индивидуально и однозначно предъявил свои идентификационные данные и выбрал одну или несколько ролей неявным либо явным образом; модуль аутентифицирует *на основе идентификации* и полномочий оператора принять выбранную роль или совокупность ролей. Действия аутентификации оператора *на основе идентификации,* выбора ролей и верификации полномочий на исполнение *предполагаемых* выбранных ролей могут быть объединены. Если криптографический модуль разрешает оператору изменять роли, то модуль должен верифицировать полномочия на исполнение *предполагаемой* выбранной роли, которая предварительно не была уполномочена.

В программном криптографическом модуле, механизм аутентификации может быть реализован операционной системой. При этом она должна отвечать требованиям данного раздела.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Криптографический модуль может разрешать аутентифицированному оператору выполнять все сервисы, предусмотренные уполномоченной ролью или может потребовать отдельной аутентификации по каждому сервису или для различных наборов сервисов. Если оператор работает с перерывами, тогда результаты предыдущих аутентификаций уничтожаются и оператору необходимо пройти повторную аутентификацию.

Криптографический модуль может потребовать различные типы аутентификационных данных для поддержки механизмов аутентификации, включая (но не ограничивая) владение паролем, PIN, криптографическим ключом или его эквивалентом; владение физическим ключом, маркером или его эквивалентом; верификацию личных характеристик (например, биометрических). Аутентификационные данные в пределах криптографического модуля должны быть защищены от несанкционированных раскрытия, модификации и замены.

Инициализация аутентификационных механизмов заслуживает особого внимания. Если криптографический модуль не содержит аутентификационные данные, используемые для аутентификации оператора при первоначальном доступе к модулю, то необходимо использовать другие методы авторизации для управления доступом к модулю и инициализацию механизмов аутентификации. Если при управлении доступом к модулю используются заданные по умолчанию данные аутентификации, то эти данные заменяются на данные первоначальной аутентификации. Заданные по умолчанию данные аутентификации не подлежат обнулению (7.8.)

Механизм аутентификации может состоять из группы механизмов с различными свойствами аутентификации, которые совместно определяют силу аутентификационных требований этого раздела. Если криптографический модуль использует криптографические функции для аутентификации оператора, то эти функции должны являться утвержденными в установленном порядке функциями. Результирующая эффективность механизма аутентификации должна соответствовать следующим спецификациям:

a) при каждой попытке использования механизма аутентификации вероятность взлома протокола аутентификации с одной попытки должна быть равна или меньше чем 1:100 000 000 (например, угадывание пароля);

b) при многократном использовании механизма аутентификации в течение одной минуты, вероятность взлома протокола аутентификации с одной попытки должна быть равна или меньше чем 1:10 000 000;

c) требования относительно силы аутентификации должны быть удовлетворены при конструировании модуля и не полагаться на документированное процедурное управление;

d) если пароли используются как механизм аутентификации, то для модуля должны быть написаны ограничения на выбор пароля, чтобы предотвратить использование слабых паролей, которые более восприимчивы к атакам (например, словарным атакам);

e) сигналы обратной связи данных аутентификации к оператору будут скрыты во время аутентификации (например, дисплей без отображения символов при вводе пароля). Вместо фактических данных аутентификации могут быть отображены незначащие символы;

f) обратная связь к оператору во время предпринятой аутентификации не ослабляет эффективность механизма аутентификации. Если используются заданные по умолчанию данные аутентификации для управления доступом к модулю для первоначальной аутентификации, то эти данные должны быть уникальными для доставленной модульной единицы.

На первом уровне безопасности можно не использовать механизм аутентификации для управления доступом к модулю.

На втором уровне безопасности необходимо использовать аутентификацию на основе роли для управления доступом к модулю.

На третьем уровне безопасности для управления доступом к модулю необходимо использовать механизмы аутентификации на основе *идентификации.*

В дополнение к требованиям третьего уровня безопасности на четвертом и пятом уровнях безопасности необходимо проводить двухфакторную аутентификацию на основе *идентификации.*

7.3.3 Сервисы

Криптографический модуль должен обеспечить оператору следующие сервисы:

a) *индикация состояния.* Вывод текущего состояния криптографического модуля (В результате происходит вывод индикаторов состояния в ответ на запрос сервиса);

b) *индикация номера версии модуля.* Вывод имени и номера версии криптографического модуля;

c) *исполнение самотестирования.* Инициализация и выполнение предпускового *самотестирования*, как это определено в 7.9.1;

d) *исполнение утвержденной в установленном порядке функции безопасности.* Исполнение не менее одной утвержденной функции *безопасности*, используемой в утвержденном режиме работы, как это определено в 7.1;

e) *обнуление.* Исполнение *обнуления*, как это определено в 7.8.6.

Криптографический модуль может обеспечить другие утвержденные в установленном порядке сервисы, в дополнение к вышеуказанным.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI

Определенные сервисы могут быть обеспечены в нескольких ролях (например, сервисы ввода ключа могут быть обеспечены в пользовательской роли и роли криптосотрудника);

f) *возможность обхода.* Способность обслуживания с частичным или полным обходом криптографической функции. Если модуль может вывести специфические данные или указатель состояния отражает результат конфигурации модуля или действия оператора, то появляется возможность обхода криптографической функции.

Если криптографический модуль реализует возможность обхода, то:

1) оператор примет уполномоченную роль перед конфигурированием возможности обхода;

2) необходимо использовать пару независимых внутренних действий дезактивизации механизмов, предназначенную для обеспечения корректного обхода функций безопасности. Пара независимых внутренних действий должна изменить поведение программного и/или аппаратного обеспечения, которые специализированы для реализации обхода;

3) выдастся индикация о состоянии модуля, которая несет в себе информацию о типе обеспечиваемых сервисов;

4) не используются криптографические функции (с активизацией возможности обхода) или

5) используются криптографические функции (без активизации возможности обхода).

g) *внешняя загрузка программ.* Если криптографический модуль имеет возможность загрузки программного обеспечения из внешнего источника, то:

1) логическая функция, выполняющая внешнюю загрузку программного обеспечения, будет логически разъединена от вывода данных;

2) криптографический модуль не реализует загрузку кода, пока тестирование загрузки программного обеспечения, указанное в 7.9.2, успешно не верифицирует подлинность загружаемого кода от внешних источников;

3) криптографический модуль не будет выполнять никакие загруженные утвержденные в установленном порядке функции безопасности, пока не завершится успешное выполнение процедуры *самотестирования криптографического алгоритма*, указанной в 7.9.1;

4) модуль поддерживает утвержденный в установленном порядке метод аутентификации для верификации подлинности загружаемого программного обеспечения.

7.4 Безопасность программного обеспечения

Требования этого подраздела относятся к программному обеспечению модулей.

К программному обеспечению криптографического модуля первого уровня безопасности предъявляются следующие требования:

a) весь криптографический код в пределах модуля должен быть в готовой к выполнению форме;

b) криптографический механизм должен использовать утвержденную в установленном порядке методику обеспечения целостности (например, утвержденный КАС или алгоритм ЭЦП) на базе криптографического ключа, применимого ко всему программному обеспечению криптографического модуля. Ключ может постоянно находиться в модуле;

c) ввод и вывод осуществляется через определенный ИПМ модуля;

d) ИПМ не допускает оператора к услуге чтения программного обеспечения;

e) ИПМ не разрешает оператору модифицировать программное обеспечение модуля, без вызова процедуры тестирования загрузки программного обеспечения, как это определено в 7.9.2;

f) любые модификации программного обеспечения модуля, отличающиеся от полной перезагрузки подлежат тестированию загрузки программного обеспечения, как это определено в 7.9.2;

g) если ожидается поступление от внешних источников специфического формата для подготовленных к вводу данных, то модуль должен верифицировать формат.

К программному обеспечению криптографического модуля второго уровня безопасности в дополнение к требованиям первого уровня безопасности предъявляется следующее требование:

- утвержденная в установленном порядке методика целостности, используемая при тестировании целостности программного обеспечения, должна состоять из процедур генерации ЭЦП с использованием утвержденного в установленном порядке алгоритма ЭЦП. Субъект, запрашивающий признания правильности, должен генерировать личный ключ для формирования кода и открытый ключ для верифицирования кода. Личный ключ ЭЦП должен находиться в пределах модуля только в течение процесса формирования ЭЦП. Открытый ключ для целей верификации может находиться вместе с кодом модуля постоянно.

К программному обеспечению криптографического модуля третьего уровня безопасности в дополнение к требованиям второго уровня безопасности предъявляются следующие требования:

a) команда ИПМ (то есть вызываемая услуга), разрешающая криптосотруднику инициализировать тестирование целостности программного обеспечения, должна быть выполнена без снижения установленного энергопотребления модулем;

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

b) команда ИПМ должна вывести индикацию последнего вычисленного хэш-значения и оценку (в виде "успешно" или "безуспешно") процедуры тестирования целостности программного обеспечения;

c) значение хэш-функции программного обеспечения модуля должно быть обнулено после завершения команды ИПМ, инициализировавшей тестирование целостности программного обеспечения.

К программному обеспечению криптографического модуля четвертого уровня безопасности в дополнение к требованиям третьего уровня безопасности предъявляются следующие требования:

a) модуль должен иметь возможность расшифровать зашифрованную часть программного обеспечения в самом начале процесса загрузки. Все КПБ, так же как программа для тестирования целостности программного обеспечения (включая открытый ключ для верификации и ЭЦП), должны быть представлены в зашифрованной форме со стороны поставщика с использованием симметричного ключа. Симметричный ключ, или ключевые компоненты, должны первоначально быть сгенерированы поставщиком (7.8.2) и транспортироваться к месту установки модуля (7.8.3 и 7.8.4). Симметричный ключ не подлежит сохранению в пределах модуля, когда модуль транспортируется клиенту. Когда программное обеспечение загружено в модуль, криптосотрудник должен ввести симметричные ключи или ключевые компоненты (7.8.4), чтобы расшифровывать зашифрованные части. Тестирование целостности программного обеспечения, включая симметричный ключ (как данные), должно быть выполнено во время предпускового тестирования;

b) прежде чем модуль переходит в предпусковое состояние, криптосотрудник должен иметь в запасе новый симметричный ключ или ключевую компоненту (иначе используется текущий симметричный ключ). КПБ и программа для тестирования целостности программного обеспечения (включая открытый ключ для верификации и ЭЦП) должны быть зашифрованы и все копии открытого текста этих значений в пределах модуля должны быть автоматически обнулены;

c) новая ключевая пара, используемая в процессе тестирования целостности программного обеспечения, и новый симметричный ключ шифрования первоначально должны быть сгенерированы (7.8.2) для каждого экземпляра этого криптографического модуля;

d) режим шифрования, используемый для защиты КПБ и программы для тестирования целостности программного обеспечения (включая открытый ключ для верификации и ЭЦП), представляет собой утвержденную в установленном порядке функцию шифрования в режиме аутентификации.

К программному обеспечению криптографического модуля пятого уровня безопасности в дополнение к требованиям четвертого уровня

безопасности предъявляется следующее требование: в дополнение ко всем КПБ и программе тестирования целостности программного обеспечения (включая открытый ключ для верификации и ЭЦП) ко всем ОПБ должно быть применено симметричное шифрование, описанное для четвертого уровня.

7.5 Операционная среда

Операционная среда криптографического модуля представляет собой совокупность всего программного обеспечения и аппаратных средств, необходимых для обеспечения безопасного функционирования модуля. Например, операционная среда программного модуля включает собственно модуль, процессор, на котором выполняется программа, и операционную систему, управляющую выполнением этой программы. Операционная среда может быть неподдающейся модификации (не модифицируемой) или поддающейся модификации (модифицируемой).

Требования этого подраздела относятся только к модулям, содержащим программное обеспечение, используемое в модифицируемой операционной среде. Эти требования не имеют отношения к любым модулям, используемым в не модифицируемой операционной среде или в отдельно выделенной аппаратной части модулей.

Не модифицируемая среда содержит только утвержденное в установленном порядке программное обеспечение. Эта среда может состоять из программного обеспечения, используемого в неперепрограммируемом компьютере (например, неперепрограммируемой карте или смарт-карте), или программного обеспечения, модернизация которого производится с использованием утвержденных в установленном порядке процессов аутентификации данных (то есть на базе процедуры тестирования загрузки программного обеспечения, указанной в 7.9.2). При этом компоненты окружающей среды, которые также являются не модифицируемыми, должны служить внешней границей для программного модуля.

Модифицируемая операционная среда позволяет загружать неутвержденное в установленном порядке программное обеспечение. Такая среда может включать общие целевые функции операционной системы (например, использование ОС компьютера или ОС конфигурируемой смарт-карты). Операционные системы считаются модифицируемыми операционными средами, если программное обеспечение может быть модифицировано оператором и/или оператор сможет загрузить и выполнить программное обеспечение (например, текстовой процессор), которое ранее не было включено в состав модуля.

В таблице 1 приведены некоторые примеры немодифицируемых и модифицируемых сред.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Таблица 1- Примеры операционных сред

Конфигурация	**Операционная среда**
Криптографический модуль не допускает загрузку ПО и не разрешает оператору модифицировать конфигурацию ОС криптографического модуля	Не модифицируемая
Криптографический модуль допускает загрузку дополнительного аутентифицированного ПО и отвечает всем требованиям данного стандарта	Не модифицируемая
ПО на компьютере не изолировано от входных данных	Модифицируемая
ПО на процессоре, который допускает ввод не действительного исполняемого кода	Модифицируемая
ПО на компьютере, ОС которого является переконфигурируемой со стороны оператора, позволяя ему исключать защитные механизмы безопасности	Модифицируемая

Требования, приведенные в 7.5.1, не относятся к немодифицируемым операционным средам.

Если операционная среда является модифицируемой, то указанные требования должны быть соблюдены. Целью нижеприведенных требований является логическая защита криптографического модуля от несанкционированного доступа, реализованная на базе модифицируемой операционной среды.

В документации должна быть указана операционная среда криптографического модуля, в которой применима используемая модулем операционная система.

7.5.1 Требования к операционной системе для модифицируемых операционных сред

На первом уровне безопасности криптографических модулей отличительными особенностями обладают только требования к операционным системам. Доступ к сервисам модуля может иметь только один среди конкурирующих операторов, который участвует лишь только в одном сеансе работы.

К операционным системам первого уровня безопасности, ограниченным единственным сеансом работы оператора в любое заданное время, предъявляются следующие требования (параллельная работа операторов, как правило, исключается):

a) все команды ИПМ в сеансе будут выполнены от имени единственного оператора;

b) все КПБ должны быть обнулены прежде, чем завершится сеанс текущего оператора и начнется сеанс нового оператора;

c) процессы, порожденные криптографическим модулем, будут принадлежать только модулю, а не внешним процессам или операторам.

Если операционная система может обеспечить параллельную работу операторов, то необходимо обеспечить выполнение следующих требований:

a) все криптографическое программное обеспечение, ЧПБ и управление информацией о состоянии должны быть под управлением операционной системы, которая осуществляет контролируемое управление доступом для обеспечения защиты от несанкционированного выполнения, модификации и чтения;

b) в целях защиты данных открытого текста криптографическое программное обеспечение, ЧПБ и аутентификационные данные, механизмы управления доступом операционной системы должны быть сконфигурированы для:

1) предписания набора ролей, которые могут исполняться с использованием криптографического программного обеспечения;

2) ввода в действие набора ролей, на основе которых можно модифицировать (то есть записывать, заменять или удалять) нижеприведенное ПО криптографического модуля, хранимого в пределах криптографической границы: криптографические программы, криптографические данные (например, криптографические данные аудита), ЧПБ и открытый текст;

3) ввода в действие набора ролей, на основе которых можно считывать программное обеспечение криптографического модуля, хранимое в пределах криптографической границы: криптографические данные (например, криптографические данные аудита), ЧПБ и открытый текст;

4) написания набора ролей, которые могут ввести ЧПБ;

c) должны быть совместимы с ролями и сервисами, как это определено в политике безопасности, следующие спецификации:

1) операционная система должна препятствовать всем операторам и выполняющимся процессам модифицировать выполняемые криптографии-ческие процессы (то есть загруженные и выполняемые криптографические программы);

2) операционная система должна препятствовать операторам получать или читать, либо иметь доступ для записи ЧПБ других операторов;

3) операционная система должна препятствовать операторам и внешним выполняемым процессам знакомиться с криптографическим

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

программным обеспечением, хранимым в пределах криптографической границы;

4) конфигурация операционной системы, соответствующая вышеупомянутым требованиям, должна быть приведена в руководстве криптосотрудника. В руководстве должно констатироваться, что операционная система должна быть сконфигурирована в указанной форме, прежде чем прийти к выводу, что содержание модуля надежно защищено.

К криптографическим модулям второго уровня безопасности, обеспечивающим параллельную работу нескольких операторов с параллельным доступом, в дополнение к требованиям первого уровня безопасности предъявляются следующие требования:

a) операционная система должна обеспечивать механизм аудита для регистрации модификаций, доступов, удалений и добавлений криптографических данных и ЧПБ. Если информация аудита хранится вне модуля, то модуль должен использовать утвержденные в установленном порядке криптографические механизмы защиты информации от несанкционированного раскрытия и модификации со стороны внешних по отношению к модулю субъектов и объектов;

b) механизмом аудита должны регистрироваться следующие события:

1) попытки совершить несанкционированный ввод функций криптосотрудником и

2) присвоение оператору роли криптосотрудника или исключение его из этой роли;

c) механизм аудита должен быть способным осуществлять аудит следующих событий:

1) доступ всех операторов для чтения и записи в целях аудита данных, хранимых в контрольной записи (выполняемых процессов),

2) запросов для использования механизмов управления аутентификационными данными,

3) использования связанных с безопасностью функций криптосотрудника,

4) запросов для доступа к аутентификационным данным, связанным с криптографическим модулем,

5) использования механизма аутентификации (например, логина), связанного с криптографическим модулем,

6) запросов для доступа к особому личному ключу,

7) явных запросов для принятия роли криптосотрудника.

В политике безопасности модуля должен быть определен используемый код для идентификации и аутентификации операторов модуля на базе кода операционной системы или кода, снабженного поставщиком. В

любом случае идентификационные и механизмы аутентификации должны отвечать требованиям 7.3.2.

К криптографическим модулям третьего уровня безопасности в дополнение к требованиям второго уровня безопасности предъявляются следующие требования:

a) операционная система должна быть сконфигурирована так, чтобы не допускать использование оператором роли пользователя (если поддерживается) модифицировать программное обеспечение криптографического модуля, системные ЧПБ и данные аудита, хранимые в пределах операционной среды модуля;

b) между аутентифицированными операторами и криптографическим модулем должен быть создан доверенный канал;

c) все ЧПБ, аутентификационные данные, вводы управления, и выводы состояния должны передаваться через доверенный канал. Связь через этот доверенный канал должна быть активизирована исключительно оператором или криптографическим модулем. Доверенный канал должен обеспечивать исходную аутентификацию и должен предотвращать несанкционированную модификацию, замену, раскрытие и воспроизведение чувствительных параметров безопасности;

d) в дополнение к требованиям аудита второго уровня безопасности механизмом аудита должны регистрироваться следующие события:

1) попытки использовать функцию доверенного канала;

2) идентификация инициатора и адресата доверенного канала.

На данном уровне безопасности должны применяться только операционные системы, которые постоянно конфигурируются для удовлетворения вышеупомянутых требований безопасности.

В дополнение к требованиям третьего уровня безопасности к четвертому и пятому уровням безопасности предъявляется следующее требование: контрольный механизм аудита должен быть постоянно конфигурирован таким образом, чтобы нижеследующие события всегда подвергались аудиту:

a) доступ оператора на чтение или запись ко всем данным аудита, хранимым в журнале аудита;

b) запросы на использование механизмов управления аутентификационными данными;

c) использование функций криптосотрудника, связанных с безопасностью;

d) запросы на доступ к механизмам аутентификации, связанным с криптографическим модулем.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

7.6 Физическая безопасность

Для исключения возможности несанкционированного физического доступа к содержанию установленного криптографического модуля, его несанкционированного использования или модификации в модуле должны быть использованы физические механизмы безопасности. Все аппаратные средства, программное обеспечение и ЧПБ в пределах криптографической границы должны быть защищены.

Требования данного подраздела применимы только к аппаратным, особым аппаратным и гибридным модулям и не имеют отношения к программным модулям.

Благодаря применению физических механизмов безопасности в модуле вероятность обнаружения попыток неавторизованного физического доступа, попыток несанкционированного использования или модификации модуля достаточно высока. Это связано, с тем, что обычно нарушитель оставляет видимые признаки попытки атаки (то есть улики вмешательства). В этих случаях во время совершения попыток атак немедленно предпринимаются ответные действия, направленные на защиту ЧПБ.

В таблице 2 приведены обобщенные требования физической безопасности для каждого из пяти уровней безопасности модулей.

Первый уровень безопасности требует минимальной физической защиты.

На втором уровне безопасности в дополнение к требованиям первого уровня требуются механизмы обнаружения явных вмешательств и сбора информации о внешних операциях по отношению к модулю.

На третьем уровне безопасности добавлены требования относительно механизмов обнаружения и реакции на вмешательства, а также защиты вентиляционных каналов от проникновения.

На четвертом уровне безопасности добавлены требование защиты от отказов вследствие воздействий окружающей среды (температуры и напряжения источника электропитания) или требование их тестирования.

На пятом уровне безопасности помимо защиты от воздействий окружающей среды (температуры и напряжения источника электропитания) добавлены требования по экспертизе непроницаемости относительно невидимой радиации, защите от электростатических разрядов и слабой радиации, а также реакции против выведения из строя модуля.

Таблица 2 - Требования по физической безопасности к аппаратным, особым аппаратным и гибридным модулям

Уровни безопасности	**Общие требования**
Первый уровень	Компоненты на промышленном уровне.
Второй уровень	Компоненты на промышленном уровне. Механизмы обнаружения явных вмешательств
Третий уровень	Компоненты на промышленном уровне. Механизмы обнаружения явных вмешательств. Реакция на вмешательство и схема обнуления. Защита вентиляционных каналов от проникновения.
Четвертый уровень	Компоненты на промышленном уровне. Механизмы обнаружения явных вмешательств. Реакция на вмешательство и схема обнуления. Защита вентиляционных каналов от проникновения. Защита от воздействий окружающей среды (температуры и напряжения источника электропитания) или тестирование на воздействия окружающей среды.
Пятый уровень	Компоненты на промышленном уровне. Механизмы обнаружения явных вмешательств. Реакция на вмешательство и схема обнуления. Защита вентиляционных каналов от проникновения. Защита от воздействий окружающей среды (температуры и напряжения источника электропитания). Проверка непроницаемости относительно невидимой радиации. Защита от электростатических разрядов и слабой радиации. Реакция на выход модуля из строя.

7.6.1 Общие требования по физической безопасности

К аппаратным и гибридным криптографическим модулям предъявляются следующие требования по физической безопасности:

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

a) документация должна содержать спецификацию и описание уровня безопасности, для которого разработаны физические механизмы безопасности криптографического модуля;

b) всякий раз, когда в целях физической безопасности производится обнуление, оно должно произойти за достаточно короткий промежуток времени. Это необходимо для обеспечения необратимости фактического обнуления;

c) если модулем поддерживается роль, разрешающая физический доступ к содержанию модуля или когда модуль разработан с учетом разрешения физического доступа (например, поставщику модуля или другому уполномоченному субъекту), тогда:

1) должен быть определен интерфейс поддержки доступа;

2) должны использоваться все физические пути доступа к содержимому модуля, включая любые съемные элементы корпуса (крышки, дверцы и т.д.);

3) когда имеет место доступ к интерфейсу поддержки доступа все КПБ (и ОПБ для пятого уровня безопасности) должны быть обнулены.

На первом уровне безопасности ко всем криптографическим модулям предъявляются следующие требования:

a) криптографический модуль должен состоять из компонентов промышленного уровня, которые должны включать стандартные методы защиты (например, специальное покрытие или применение защитного слоя над схемой модуля, защита от воздействий окружающей среды или другого повреждения физической природы);

b) при выполнении физического обслуживания все КПБ модуля должны быть обнулены. Обнуление должно быть выполнено процедурно оператором или автоматически криптографическим модулем.

На втором уровне безопасности в дополнение к требованиям первого уровня безопасности к криптографическим модулям предъявляются следующие требования:

a) при попытке физического доступа к модулю должны появляться признаки вмешательства (например, на покрытии, корпусе или печати);

b) при конструировании должна быть исключена возможность утечки информации за счет прямого визуального наблюдения через имеющиеся вентиляционные отверстия и щели с помощью внутренних искусственных источников света или компонентов модуля.

На третьем уровне безопасности в дополнение к требованиям первого и второго уровня безопасности, к криптографическим модулям предъявляются следующие требования:

a) при наличии в криптографическом модуле вентиляционных отверстий и щелей должны быть предусмотрены механизмы обнаружения

утечки информации за счет прямого визуального наблюдения посредством искусственных источников света, а также модуль должен содержать механизмы реагирования на вмешательства и схему обнуления, которые должны приводиться в действие немедленно при попытках открыть дверцы, удалении покрытий, или когда обращаются к интерфейсу поддержки доступа. Механизмы реагирования на вмешательство и схема обнуления должны оставаться в рабочем режиме до тех пор, пока в криптографическом модуле существует КПБ;

b) при наличии в криптографическом модуле вентиляционных отверстий и щелей они должны быть сконструированы таким образом, чтобы попытки зондирования всегда обнаруживались.

На четвертом уровне безопасности в дополнение к требованиям первого, второго и третьего уровней безопасности к криптографическим модулям предъявляются следующие требования:

a) криптографический модуль должен быть защищен либо твердым непрозрачным покрытием, стойким к удалению, либо корпусом и иметь механизмы обнаружения вмешательств, реагирования и обнуления;

b) модуль должен иметь защиту от воздействий окружающей среды или подвергаться тестированию на воздействия окружающей среды.

На пятом уровне безопасности в дополнение к требованиям первого, второго, третьего и четвертого уровней безопасности к криптографическим модулям предъявляются следующие требования:

a) в криптографическом модуле должна быть предусмотрена защита от воздействий окружающей среды (температуры и напряжения электропитания);

b) криптографический модуль должен быть непрозрачным к невидимому лучевому сканированию (например, рентгеновским лучам, тепловому отражению и т.д);

c) криптографический модуль должен обеспечивать защиту от электростатических разрядов и электромагнитной индукции, которые приводят к нарушениям работоспособности.

7.6.2 Защита от воздействий окружающей среды/Тестирование

Электронные устройства разрабатываются для работы в определенном диапазоне параметров окружающей среды. Преднамеренные или случайные изменения этих параметров, выходящие за пределы определенных нормальных диапазонов рабочих напряжения и температуры, могут привести к нарушению функционирования или выходу из строя электронных устройств или схем, что может поставить под угрозу безопасность криптографического модуля. Гарантию того, что безопасность криптографического модуля не может быть скомпрометирована чрезвычайными воздействиями окружающей

...ENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

среды, можно обеспечить с помощью защиты от воздействий окружающей среды или подвергая модуль тестированию на воздействия окружающей среды.

На первом, втором и третьем уровнях безопасности для криптографического модуля не используется защита от воздействий окружающей среды и модуль не подвергается тестированию на воздействия окружающей среды.

На четвертом уровне безопасности криптографический модуль должен либо использовать защиту от воздействий окружающей среды, либо подвергаться тестированию на воздействия окружающей среды.

На пятом уровне безопасности в криптографическом модуле должна быть реализована защита от воздействий окружающей среды, а именно температуры и напряжения.

7.6.2.1 Особенности безопасности окружающей среды

Особенности защиты от воздействий окружающей среды позволяют защитить криптографический модуль от необычной окружающей среды или колебаний (случайных изменений или индукций) за пределами рабочего диапазона изменений для модуля, который может ставить под угрозу безопасность модуля.

Криптографический модуль должен контролировать и правильно реагировать на колебания рабочей *температуры* и *напряжения* за пределами нормальных рабочих диапазонов.

Защита от воздействий окружающей среды должна быть реализована на электронных схемах или устройствах, которые непрерывно измеряют температуру и напряжение криптографического модуля. Если температура или напряжение выходят за пределы нормального рабочего диапазона значений, то схемы защиты должны отключить модуль, чтобы предотвратить дальнейшее воздействие, или немедленно обнулить все КПБ и ОПБ.

Нормальные рабочие диапазоны и особенности защиты от воздействий окружающей среды криптографичеекого модуля должны быть отражены в документации.

7.6.2.2 Процедура тестирования на воздействия окружающей среды

Тестирование на воздействия окружающей среды должно включать процедуры анализа, моделирования и испытания криптографического модуля, чтобы обеспечить разумную гарантию того, что воздействия окружающей среды (случайные или индукционные) за пределами рабочего диапазона изменений температуры и напряжения для модуля, его не скомпрометируют.

Тестирование на воздействия окружающей среды должно продемонстрировать, что если текущие значения температуры или напряжения выходят за пределы рабочего диапазона, вследствие чего может произойти отказ в работе, то криптографический модуль никогда не будет скомпрометирован.

Тестирование температурного диапазона осуществляется в следующем порядке:

a) тестируемая температура постепенно снижается относительно нижнего предела нормального диапазона к еще более низкому значению, в результате чего модуль должен либо отключиться (1) и прекратить дальнейшее функционирование, либо должны немедленно обнулиться все КПБ, а также ОПБ, если процедура тестирования осуществляется для пятого уровня безопасности (2);

b) тестируемая температура постепенно увеличивается относительно верхнего предела нормального температурного диапазона к еще более высокому значению, в результате чего модуль должен либо отключиться (1) и прекратить дальнейшее функционирование, либо должны немедленно обнулиться все КПБ, а также ОПБ, если процедура тестирования осуществляется для пятого уровня безопасности (2).

Тестируемый диапазон температуры должен быть от минус 100°C до плюс 200°C (от минус 150°F до плюс 400°F); однако, испытание должно быть прервано, как только произойдет любой из следующих исходов: (1), (2) или (3). Здесь, исход (3) соответствует событию перехода модуля в состояние отказа от функционирования.

Аналогично с описанным проводится тестирование диапазона изменений напряжения источника питания:

a) тестируемое напряжение постепенно снижается относительно нижнего уровня напряжения в пределах нормального диапазона изменений напряжения к более низкому значению, в результате чего модуль должен либо отключиться (1) и прекратить дальнейшее функционирование, либо немедленно должны обнулиться все КПБ, а также ОПБ, если процедура тестирования осуществляется для пятого уровня безопасности (2);

b) тестируемое напряжение постепенно повышается относительно верхнего уровня напряжения в пределах нормального диапазона изменений напряжения к более высокому значению, в результате чего (1) модуль должен либо отключиться и прекратить дальнейшее функционирование, либо немедленно должны обнулиться все КПБ, а также ОПБ, если процедура тестирования осуществляется для пятого уровня безопасности (2).

Нормальные рабочие диапазоны работы криптографического модуля и порядок оформления результатов тестирования на воздействия окружающей среды должны быть определены в документации.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, MUVOFIQLASHTIRISH VA DAVLAT NAZORATI BOSHQARMASI

7.7 Защита от неразрушающих атак

В данном подразделе определены физические (не логические) атаки нарушителей на рабочий процесс модуля, которые не требуют физического контакта или непосредственного обследования модуля. К неразрушающим атакам относятся атаки на основе упрощенного анализа мощности, дифференциального анализа мощности, электромагнитного излучения, временного анализа. Могут существовать другие виды неразрушающих атак, однако защита от них в настоящее время на всех уровнях безопасности считается необязательной.

На первом и втором уровнях безопасности криптографических модулей защита от неразрушающих атак, перечисленных в данном разделе, не используется.

На третьем уровне безопасности криптографического модуля КПБ модуля должны быть защищены от атак на основе ВА.

Методы подавления проводимых атак на основе ВА должны быть описаны в документации.

На четвертом уровне безопасности криптографического модуля дополнительно к требованиям безопасности третьего уровня безопасности ко всем криптографическим модулям должны быть предъявлены следующие требования:

a) криптографический модуль должен защищать КПБ от атак на основе УАМ. Методы подавления проводимых атак на основе УАМ мощности должны быть определены в документации;

b) криптографический модуль должен защищать КПБ от атак на основе ДАМ. Методы подавления проводимых атак на основе ДАМ должны быть определены в документации.

Ко всем криптографическим модулям пятого уровня безопасности дополнительно к требованиям безопасности четвертого уровня безопасности должно предъявляться следующее требование: криптографический модуль должен защищать КПБ от атак на основе электромагнитных излучений.

Методы подавления проводимых атак на основе дифференциального ЭМИ должны быть определены в документации.

7.8 Управление чувствительными параметрами безопасности

К чувствительным параметрам безопасности относятся открытые и критичные параметры безопасности, включая особый личный ключ, встраиваемый в особый аппаратный модуль на стадии разработки или регистрации открытых ключей. Требования безопасности к управлению ЧПБ охватывают весь жизненный цикл ЧПБ, используемых модулем. Управление

Если используется особый аппаратный модуль, то процедура встраивания в модуль осуществляется в строгом соответствии с руководством для уполномоченного субъекта лишь только на стадии разработки или регистрации открытых ключей.

7.8.4 Ввод и вывод чувствительного параметра безопасности

Ввод или вывод из модуля ЧПБ (за исключением особого личного ключа) могут быть осуществлены только уполномоченными субъектами. Ввод или вывод ЧПБ выполняется с использованием ручных (например, вводятся с помощью клавиатуры или выводятся на дисплее) или электронных (например, посредством смарт-карт/токенов, карт персональных компьютеров, других устройств загрузки ключей, модульных операционных систем) методов или их комбинаций.

Применяемые методы ввода и вывода ЧПБ должны быть описаны в документации, где особо должно быть подчеркнуто, что полномочия ввода и вывода особого личного ключа принадлежат только уполномоченному субъекту с особым личным ключом. Модуль должен связывать введенный в модуль или выведенный из модуля ЧПБ (за исключением особого личного ключа) с соответствующим субъектом (например, лицом, группой, ролью, или процессом), для которого назначен ЧПБ.

Все введенные или выведенные зашифрованные ЧПБ, используемые в утвержденном в установленном порядке режиме работы, должны быть зашифрованы с использованием утвержденных в установленном порядке функций безопасности.

Во время ввода ЧПБ вручную (за исключением особого личного ключа), вводимое значение может быть временно выведено на экран дисплея, чтобы для повышения точности ввода производить визуальную проверку. Если зашифрованные КПБ вводятся в модуль вручную, тогда открытый текст КПБ не должен выводиться на экран. Вводимые вручную (зашифрованные или незашифрованные) криптографические ключи, включая начальные ключи, должны быть проверены во время ввода в модуль на точность с использованием теста ручного ввода ключа, определенного в 7.9.2.

Для программных модулей КПБ могут быть введены или выведены из модуля в зашифрованном или в незашифрованном виде под контролем операционной системы модуля, чем обеспечивается фиксирование КПБ в пределах рабочей среды. ОПБ могут быть введены или выведены из модуля в незашифрованном виде.

Электронно-транспортируемые КПБ должны вводиться и выводиться из модуля в зашифрованной виде, а также должна быть обеспечена их целостность (например, посредством утвержденных в установленном порядке функций безопасности или утвержденного в установленном порядке метода

O'ZBEKISTON STANDARTLASHTIRISH, MUVOFIQLASHTIRISH VA DAVLAT NAZORATI AGENTLIGI

установки ключа). Электронно-транспортируемые ОПБ должны вводиться и выводиться из модуля, обеспечивая гарантированную целостность с помощью утвержденного в установленном порядке алгоритма ЭЦП или утвержденного в установленном порядке КАС, либо утвержденным в установленном порядке методом транспортировки.

Для первого и второго уровней безопасности не предъявляется никаких дополнительных требований безопасности.

Для третьего, четвертого и пятого уровней безопасности транспортируемые КПБ без использования электронных средств должны быть введены или выведены из модуля либо в зашифрованном виде (1), либо с использованием процедуры разделения знаний (например, на два или более зашифрованных компонентов). Если используется процедура разделения знаний, то:

a) модуль должен аутентифицировать оператора, вводящего или выводящего каждую компоненту, как отдельную личность;

b) модуль должен проверять, имеются ли у двух операторов (вводящих или выводящих ключевые компоненты) разные идентификаторы;

c) для предотвращения неправильного использования ЧПБ криптографический модуль должен использовать доверенный канал для ввода или вывода всех ЧПБ (за исключением особого личного ключа) независимо от того, защищены они криптографически или нет. Если доверенный канал установлен и поддерживается криптографическими алгоритмами, то алгоритмы должны являться утвержденными в установленном порядке и обладать стойкостью безопасности модуля, указанной в документации;

d) необходимо использовать, по крайней мере, часть ключа для восстановления оригинала КПБ (за исключением особого личного ключа);

e) в документации должно быть указано, что если необходимо знание *n* компонентов для восстановления оригинала КПБ (за исключением особого личного ключа), тогда знание любых *n-1* компонентов не дает никакой информации об оригинале КПБ, кроме его длины;

f) в документации должна быть описана применяемая процедура разделения знаний;

g) в документации должна быть описана процедура встраивания особого личного ключа, применяемая стадия и требования к уполномоченному субъекту, исполняющую данную процедуру.

7.8.5 Хранение чувствительного параметра безопасности

ЧПБ, хранимые в модуле, могут храниться в виде открытого текста или в зашифрованном виде. Модуль должен связывать каждый ЧПБ, хранимый в модуле, с соответствующим субъектом (то есть с оператором, ролью или процессом), которому предназначен ЧПБ. ЧПБ также может храниться

внутри встроенного криптографического модуля, который удовлетворяет требованиям стандарта относительно сложных модулей.

В документации должны быть определены:

a) ЧПБ, хранимые в модуле;

b) защита КПБ от несанкционированного доступа при хранении в модуле;

c) защита ОПБ от несанкционированной модификации при хранении внутри модуля;

d) связь ОПБ, хранимого в модуле, с субъектом (оператором, ролью или процессом), которому назначен этот параметр;

e) защита особого личного ключа от несанкционированного доступа при хранении в модуле.

ОПБ и открытый текст КПБ не должны быть доступны для неуполномоченных операторов из внешней среды модуля.

Открытый текст особого личного ключа должен быть не доступен никакому другому субъекту, за исключением уполномоченного субъекта.

7.8.6 Обнуление чувствительного параметра безопасности

В модуле должны быть использованы методы обнуления всех КПБ (включая временно-хранимые значения) внутри модуля. При этом обнуленному КПБ должно быть присуще свойство не восстанавливаемости. Не требуется обнуление ОПБ, зашифрованных КПБ или КПБ внутри дополнительного встроенного утвержденного в установленном порядке модуля (удовлетворяющего требованиям данного стандарта) ниже пятого уровня безопасности. Ключи, используемые для предпускового самотестирования, должны рассматриваться как ОПБ. Хэш-значения паролей (если известны), которые могут быть объектом атаки методом перебора, должны рассматриваться как КПБ. Информация о состоянии ГСБП должна рассматриваться как КПБ.

В документации должен быть определен метод обнуления КПБ, применяемый модулем, и обоснование того, что этот метод предотвращает восстановление или повторное использование обнуленных КПБ; метод обнуления особого личного ключа может быть сведен к замене истинного значения единичным значением.

Временные КПБ (например, эфемерные ключи), если они больше не используются, должны обнуляться.

На первом и втором уровнях безопасности обнуление КПБ может быть выполнено процедурно и независимо от управления модуля, например, при переформатировании жесткого диска, уничтожении модуля во время повторного ввода из-за воздействий окружающей среды.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

На третьем уровне безопасности криптографический модуль должен управлять обнулением КПБ.

Дополнительные требования безопасности к четвертому уровню безопасности отсутствуют.

На пятом уровне безопасности должны выполняться следующие требования безопасности:

a) все ОПБ (включая, временно хранимые значения) внутри модуля должны быть обеспечены методами обнуления;

b) в документации должны быть описаны применяемые методы обнуления ОПБ и обоснование того, по какой причине и каким образом метод предотвращает восстановление или повторное использование обнуленных данных;

c) не используемые временные ОПБ должны быть обнулены.

7.9 Самотестирование

Криптографический модуль должен выполнять предпусковое самотестирование, условное самотестирование, и, если это применимо, тестирование критичных функций. Предпусковое самотестирование должно успешно завершаться до того, как модуль начнет обеспечивать какие-либо сервисы. Условное самотестирование проводится с использованием применяемых функций безопасности в полном объеме применительно к модулям программного, гибридного и аппаратного типа, в сокращенном объеме - применительно к особому аппаратному модулю. Криптографический модуль может выполнять другие тесты дополнительно к тестам, определенным в данном стандарте. При проведении процедуры тестирования особого аппаратного модуля используются параметры для тестирования, приведенные в документации.

Если самотестирование завершится безуспешно, то модуль должен зафиксировать состояние ошибки и должен вывести индикацию признак ошибки на интерфейс вывода информации об ошибке. Криптографический модуль не должен выполнять какие-либо криптографические операции или вывод данных через интерфейс вывода данных до тех пор, пока он находится в неисправном состоянии. Криптографический модуль не должен использовать какие-либо функциональные возможности, которые зависят от функции или алгоритмов, являющихся причиной безуспешного самотестирования до тех пор, пока соответствующее самотестирование не будет продолжено и будет пройдено успешно.

В документации должны быть определены:

a) самотестирование, выполняемое криптографическим модулем;

b) состояние неисправности, которое криптографический модуль может зафиксировать, если самотестирование закончилось безуспешно;

c) условия и действия, необходимые для выхода из неисправного состояния и возобновления нормальной работы криптографического модуля (например, техническое обслуживание модуля, восстановление электропитания модуля, автоматическое возобновление работы модуля, возврат модуля поставщику для ремонта).

7.9.1 Предпусковое самотестирование

Предпусковое самотестирование криптографического модуля должно проводиться в период времени между включением электропитания криптографического модуля (если модуль выключен или не задействован) и началом его функционирования и предоставления сервисов с использованием протестированных функций. До использования функций безопасности предпусковое самотестирование этих функций должно быть успешно пройдено. Предпусковое самотестирование должно быть инициализировано автоматически без вмешательства оператора. Поставщик должен установить критический период, определяющий максимальное время функционирования до повторенного предпускового самотестирования. После завершения предпускового самотестирования результаты (то есть показания об успешном или безуспешном завершении) могут быть выведены через интерфейс вывода результатов тестирования. Если модуль не выводит сообщение об ошибке при безуспешном самотестировании модуля, то оператор модуля должен иметь возможность определить с помощью процедур, приводимых в политике безопасности, что модуль зафиксировал ошибку.

Операторы должны иметь возможность периодически запускать предпусковое самотестирование модуля.

Частота предпускового самотестирования криптографического модуля должна быть определена в его документации.

В документации должны быть также определены период времени и политика относительно прерывания (прекращения) работы модуля.

Криптографический модуль должен выполнять следующие виды предпускового самотестирования: тестирование целостности программного обеспечения, тестирование криптографического алгоритма, предпусковое тестирование обхода.

Тестирование целостности программного обеспечения: ко всему достоверному программному обеспечению криптографического модуля при включении модуля должен запускаться тест с использованием утвержденных в установленном порядке методов аутентификации данных. Предпусковое самотестирование должно быть завершено до того, как криптографический модуль начнет предоставлять какие-либо сервисы. Если целостность

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

исполнительного кода (рабочей программы) не может быть проверена, то тестирование целостности программного обеспечения завершится безуспешно.

На первом уровне безопасности, утвержденные в установленном порядке методы аутентификации данных должны включать использование кода аутентификации сообщения или ЭЦП.

На остальных уровнях безопасности утвержденные в установленном порядке методы аутентификации данных должны использовать ЭЦП.

Тестирование криптографического алгоритма: этот тест проводится для всех утвержденных в установленном порядке криптографических алгоритмов (например, для зашифрования, дешифрования, аутентификации данных и генерации случайных чисел), реализованных в криптографическом модуле посредством следующих методов:

a) тест, основанный на заранее известных результатах, включает работу криптографического алгоритма над данными, для которых уже известны соответствующие выходные данные и этот криптографический алгоритм сравнивает вычисленные данные с ранее сгенерированными выходными данными. Если вычисленные данные не совпадают с заранее известными результатами, то данный тест считается безуспешным. Криптографические алгоритмы, выходные данные которых не меняются для определенного набора входных данных, должны тестироваться с помощью теста, основанного на заранее известных результатах;

b) криптографические алгоритмы с открытым ключом, выходные данные которых различны для определенного набора входных данных (например, алгоритмы ЭЦП), должны тестироваться с использованием теста, основанного на заранее известных результатах, если случайное число позволяет зафиксировать изменения выходных данных или должны тестироваться с использованием теста двухточечного согласования (7.9.2) с фиксированной парой открытого и закрытого ключа;

c) если криптографический модуль включает в себя две независимые реализации одного и того же криптографического алгоритма, тогда модуль должен:

1) непрерывно сравнивать выходные данные двух реализаций и, если выходные данные не совпадают, то тестирование с помощью теста криптографического алгоритма считается безуспешным;

2) выполнять тест, основанный на заранее известных результатах для каждого тестируемого алгоритма и режима в соответствии с определенными условиями. Не требуется тест, основанный на заранее известных результатах, для функций безопасности в утвержденном в установленном порядке методе аутентификации данных, используемых в

процессе тестирования с помощью теста целостности программного обеспечения.

Предпусковое тестирование обхода: если криптографический модуль реализует возможности обхода, тогда модуль должен гарантировать корректность управления подключением возможности обхода. Этот тест должен выполняться до использования возможности обхода.

7.9.2 Условное самотестирование

Условные тесты в полном объеме должны быть выполнены криптографическими модулем программного, гибридного и аппаратного типа для следующих видов тестов: тест двухточечного согласования, тест загрузки программного обеспечения, тест ручного ввода ключа, непрерывный тест ГСБП, тестирование источника энтропии ГСБП, условное обходное тестирование. Над особым аппаратным модулем должны быть выполнены тесты загрузки программного обеспечения и ручного ввода ключа, а также непрерывный тест ГСБП

Тест двухточечного согласования (для открытых и закрытых ключей): если криптографический модуль генерирует открытый и закрытый ключ, тогда согласно тесту двухточечного согласования для сгенерированных открытых и закрытых ключей тестирование должно выполняться следующим образом:

a) если ключи используются для выполнения транспортировки ключа, тогда зашифровывается открытый текст с использованием открытого ключа. Шифротекст сравнивается с оригиналом открытого текста. Если значения равны, то тест считается безуспешным. Если два значения различны, тогда с использованием закрытого ключа расшифровывается зашифрованный текст и полученный результат сравнивается со значением открытого текста. Если значения не равны, то тест считается безуспешным;

b) если ключи используются для вычисления и проверки ЭЦП, тогда согласованность ключей должна тестироваться с полным вычислением и проверкой ЭЦП. Если результат верификации ЭЦП безуспешно, то тест считается безуспешным;

c) если ключи используются для проверки согласованности ключей, тогда достоверность ключей должна быть протестирована посредством проверки корректной математической связи между значениями открытого и закрытого ключа.

Тест загрузки ПО: если программное обеспечение может быть загружено в криптографический модуль из внешнего источника, тогда тестирование должно проводиться следующим образом:

a) должен быть использован утвержденный в установленном порядке метод ЭЦП ко всему верифицированному программному обеспечению, загружаемому в крипто-графический модуль;

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
NUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHBARMASI

b) должны быть успешно верифицированы применяемые утвержденные в установленном порядке методы аутентификации данных;

c) перед использованием недавно загруженного программного обеспечения должны быть выполнены требования 7.9.1.

Тест ручного ввода ключа: если криптографические ключи или ключевые компоненты вводятся в криптографический модуль вручную или если происходят ошибки некорректного ввода со стороны оператора-человека, тогда должны быть выполнены следующие тесты ввода ключа вручную:

a) криптографические ключи или ключевые компоненты должны иметь код обнаружения ошибок или они должны вводиться вместе с дубликатом;

b) если используется КОО, то он должен иметь минимальную длину, равную 32 bit;

c) если КОО не может быть проверен или введенный дубликат не соответствует, то тест считается безуспешным.

Непрерывный тест ГСБП: если криптографический модуль использует утвержденный в установленном порядке ГСБП или источник энтропии ГСБП в утвержденном в установленном порядке режиме работы, то модуль должен выполнять следующий тест над каждым ГСБП и источником энтропии ГСБП, который проверяет подлинность начального его значения: если при каждом вызове ГСБП вырабатываются блоки меньшей длины чем 64 bit, то первый блок длиной n bit, сгенерированный после включения электропитания, инициализации или перезагрузки (для некоторых $n > 63$), не должен быть использован, но должен быть сохранен для сравнения со следующими сгенерированными последовательностями из n bit. Каждая последующая сгенерированная последовательность из n bit должна сравниваться со следующей такой же сгенерированной последовательностью. Тест считается безуспешным, если любые из двух последовательностей из двух блоков совпадают.

Тест источника энтропии ГСБП: если источник энтропии ГСБП содержится в рабочей среде, тогда для каждого из выходных данных источника энтропии должна быть выполнена оценка минимальной энтропии. Этот тест считается безуспешным, если оцениваемая минимальная энтропия меньше чем минимум энтропии, требуемой утвержденным в установленном порядке ГСБП.

Тест условного обхода: если криптографический модуль содержит информацию, которая управляет возможностью обхода, тогда модуль должен проверять целостность управляющей информации посредством утвержденного в установленном порядке метода обеспечения целостности предыдущей управляющей информации и должен сгенерировать новое достоверное значение с использованием утвержденного в установленном

порядке метода обеспечения целостности, следующего после предыдущей модификации. В документации должен быть определен механизм или логическое управление возможности обхода.

7.10 Гарантия жизненного цикла

Гарантия жизненного цикла имеет отношение к использованию передового опыта и технологий поставщиком криптографического модуля в процессе разработки, реализации и функционирования криптографического модуля; таким образом, гарантируется, что модуль разработан соответствующим образом, протестирован, сконфигурирован, доставлен и установлен и что имеется соответствующее руководство по эксплуатации. Устанавливаются требования к управлению конфигурацией, проектированию, к модели конечного автомата, разработке, тестированию, доставке и функционированию и к руководству по эксплуатации.

7.10.1 Управление конфигурацией

Управление конфигурацией определяет требования к системе управления конфигурацией, реализуемой поставщиком криптографической системы, к обеспечению гарантии целостности криптографического модуля. Целью СУК является предотвращение случайной или несанкционированной модификации и обеспечение возможности оперативного контроля криптографического модуля и его документации.

На первом и втором уровнях безопасности к криптографическому модулю должны применяться следующие требования безопасности:

a) для криптографического модуля и его компонентов система управления конфигурацией должна быть реализована в пределах криптографической границы и в соответствие с требованиями документации модуля;

b) каждая версия каждого элемента конфигурации (например, криптографического модуля, части аппаратного обеспечения модуля, программных компонентов модуля, ЯОАО модуля, руководства пользователя, политики безопасности и т.д.), которая входит в состав модуля и его документации, должна быть определена и классифицирована с помощью уникального идентификационного номера;

c) в течение утвержденного в установленном порядке жизненного цикла криптографического модуля СУК должна сохранять измененные идентификации и версии или пересматривать каждый элемент конфигурации;

d) СУК, используемая криптографическим модулем, должна быть определена и описана в документации.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Для остальных уровней безопасности дополнительно к требованиям для первого и второго уровней безопасности предъявляется следующее требование: элементы конфигурации СУК должны управляться автоматически.

7.10.2 Проектирование

Проектирование – это инженерное решение, которое предназначено для функционального описания криптографического модуля. Проектирование нацелено на обеспечение гарантии соответствия функциональной характеристики криптографического модуля функции, описываемой в политике безопасности.

Реализованные функции спроектированного криптографического модуля должны подвергаться процедуре тестирования вместе со всеми возможными сервисами согласно этому стандарту.

На первом уровне безопасности к криптографическому модулю предъявляется следующее требование: в документации должно быть определено соответствие между спроектированным аппаратным обеспечением и/или программным обеспечением модуля и политикой безопасности криптографического модуля, а также МКА.

На втором уровне безопасности в дополнение к требованиям первого уровня безопасности предъявляется следующее требование: в документации должны быть четко определены функциональные характеристики (в неформальной форме), внешние физические порты и логические интерфейсы криптографического модуля, цели использования физических портов и интерфейсов.

На третьем уровне безопасности в дополнение к требованиям первого и второго уровней безопасности предъявляется следующее требование: в документации должны быть приведены подробности проектирования с описаниями внутренних возможностей основных компонентов криптографического модуля, внутренние аппаратные и программные компоненты, цели аппаратных и программных компонентов и вся информация, обрабатываемая внутри криптографического модуля (в пределах криптографического модуля и основных компонентов)

На четвертом уровне безопасности в дополнение к требованиям первого, второго и третьего уровней безопасности предъявляется следующее требование: в документации должны быть определены неформальные испытания (включая предварительные и приемо-сдаточные) на соответствие проекта криптографического модуля функциональной спецификации.

На пятом уровне безопасности в дополнение к требованиям первого, второго, третьего и четвертого уровней безопасности предъявляются следующие требования:

a) в документации должна быть определена формальная модель, которая описывает правила, нормы и характеристики политики безопасности криптографического модуля. Формальная модель должна быть определена с использованием формального языка описания, то есть строгой нотации, основанной на современной математике (например, теории множеств или алгебры логики);

b) в документации должно быть приведено логическое обоснование полноты формальной модели по отношению к политике безопасности криптографического модуля;

c) документация должна содержать неформальное обоснование соответствия формальной модели с функциональными характеристиками.

7.10.3 Модель конечного автомата

Функционирование криптографического модуля должно быть определено на основе модели конечного автомата (или эквивалента), представляемой с помощью диаграмм и/или таблиц переходов состояний, а также описаний состояний. МКА должна быть достаточно детализированной, пригодной для наглядного анализа степени соответствия криптографического модуля всем требованиям данного стандарта.

Документация МКА (или эквивалента) должна включать использованные диаграммы и/или таблицы перехода состояний и описание, в которых должны быть определены:

a) рабочие состояния и состояния ошибки криптографического модуля;

b) соответствующий переход из одного состояния в другое;

c) события ввода данных, включающие ввод данных и управление вводом, которые являются причиной перехода из одного состояния в другое;

d) события вывода данных, включающие внутренние состояния модуля, вывод данных и статус выходных данных, являющихся результатом перехода из одного состояние в другое.

МКА криптографического модуля должна включать в себя следующие рабочие состояния и состояния ошибки:

a) *состояние включенного/отключенного питания*: состояние, при котором модуль находится в режиме готовности или выключен; режим электропитания: первичный, вторичный или резервный источник;

b) *состояние общей инициализации*: состояние, в котором криптографический модуль инициализирует сервисы, не являющиеся криптографическими;

c) *состояние (режим) криптосотрудника*: состояние, в котором выполняются сервисы криптосотрудника (например, криптографическая инициализация, безопасное управление и управление ключами);

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

d) *состояние ввода КПБ*: состояние для ввода КПБ в КМ;

e) *состояние (режим) пользователя* (если реализована роль пользователя): режим, при котором авторизованный пользователь выполняет сервисы безопасности, криптографические операции или другие утвержденные в установленном порядке функции;

f) *утвержденное состояние (режим)*: состояние, в котором выполняются функции безопасности;

g) *состояние (режим) самотестирования*: состояние, в котором криптографический модуль выполняет самотестирование;

h) *состояние ошибки*: состояние, в котором криптографический модуль сталкивается с ошибочным состоянием (например, безуспешное самотестирование или попытка расшифрования без рабочих ключей или КПБ). В результате одного состояния ошибки модуля могут возникнуть одно или несколько ошибочных состояний. Состояния ошибки могут включать аппаратные ошибки, которые указывают на неисправную работу оборудования, обслуживания или отладки криптографического модуля или обратимые программные ошибки, для устранения которых может потребоваться инициализация или перезагрузка модуля. Должна существовать возможность выхода из состояний ошибки, за исключением тех случаев, когда при наличии аппаратных ошибок требуются ремонт, обслуживание или отладка криптографического модуля.

7.10.4 Разработка

Корректный процесс разработки должен обеспечивать гарантию, что реализация криптографического модуля соответствует его функциональным характеристикам и политике безопасности, что утвержденный в установленном порядке криптографический модуль пригоден для ремонта и воспроизводим. Этот пункт определяет требования безопасности для представления характеристик безопасности криптографического модуля на различных уровнях абстракции, начиная от функциональных характеристик вплоть до реализации.

На первом уровне безопасности КМ должен соответствовать следующим требованиям:

a) если криптографический модуль содержит программное обеспечение, то в документации должны быть определены компиляторы, установочные параметры конфигурации и методы для компиляции исходного кода в исполняемую форму. Документация также должна включать в себя исходный код программного обеспечения, аннотированный комментариями, которые описывают соответствие программного обеспечения проекту модуля;

b) если криптографический модуль содержит аппаратное обеспечение, то документация должна содержать схемы или язык описания аппаратного

обеспечения в виде приложения. ЯОАО должен аннотироваться комментариями, которые описывают соответствие аппаратного обеспечения проекту модуля.

На втором и третьем уровнях безопасности дополнительно к требованиям безопасности первого уровня безопасности к криптографическим модулям должны применяться следующие требования:

a) всё программное обеспечение криптографического модуля должно быть реализовано с использованием высокоуровневого языка, за исключением использования низкоуровневого языка (например, языка ассемблера или микрокода), если это необходимо для качественного функционирования модуля или если высокоуровневые языки не применимы;

b) индивидуальные интегрированные цепи внутри криптографического модуля должны быть реализованы с использованием высокоуровневого ЯОАО.

На четвертом и пятом уровнях безопасности дополнительно к требованиям безопасности первого, второго и третьего уровней безопасности к криптографическим модулям выставляется следующее требование: для каждого аппаратного или программного компонента криптографического модуля документация должна быть аннотирована комментариями, которые должны быть определять (1) предварительные условия, необходимые для корректного исполнения компонентов, функций или процедур модуля и (2) выходные условия (постусловия), которые станут верными после завершения исполнения компонентов, функций или процедур модуля. Предварительные условия и постусловия должны быть описаны с использованием нотации, которая достаточно детализирована для полного и однозначного объяснения поведения компонентов, функций и процедур криптографического модуля.

Если для всех или некоторых уровней безопасности разработаны особые аппаратные модули, то уполномоченный субъект должен сгенерировать соответствующие особые личные ключи с использованием ГСБП и реализовать процедуру встраивания особого личного ключа в соответствующие модули.

7.10.5 Тестирование криптографического модуля поставщиком

В этом пункте определены требования безопасности для проведения тестирования криптографического модуля поставщиками, включая тестирование характеристик безопасности, реализованных в криптографическом модуле, обеспечивающие гарантию того, что модуль работает в соответствии с его политикой безопасности и функциональными характеристиками.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
DEPARTAMENTI

Для первого и второго уровней безопасности в документации должна быть определена процедура функционального тестирования криптографического модуля.

Функциональное тестирование - тестирование характеристик криптографического модуля должно производиться в соответствие с функциональными спецификациями, описанными в 7.10.2.

Для третьего, четвертого и пятого уровней безопасности дополнительно к требованиям первого и второго уровней безопасности в документации должны быть определены процедуры для выполнения и получения результатов низкоуровневого тестирования криптографического модуля.

Низкоуровневое тестирование - это тестирование отдельных компонентов или групп компонентов криптографического модуля, их физических портов и логических интерфейсов должно производиться в соответствие с документацией для третьего уровня безопасности (7.10.2).

7.10.6 Доставка и презентация

В этом пункте определены требования безопасности к безопасной доставке, инсталляции и презентации функционирования (запуску) криптографического модуля, гарантирующие, что модуль доставлен уполномоченным операторам безопасно, корректно безопасно инсталлирован и процедуры встраивания особого личного ключа в особый аппаратный модуль (если используется аппаратный модуль) выполнены безопасным образом.

Для первого уровня безопасности в документации должны быть определены процедуры для безопасной инсталляции, инициализации и запуска криптографического модуля.

На втором уровне безопасности дополнительно к требованиям безопасности первого уровня безопасности в документации должны быть определены процедуры, необходимые для поддержания безопасности во время распространения и доставки версий криптографического модуля авторизованным операторам.

На третьем, четвертом и пятом уровнях безопасности дополнительно к требованиям безопасности второго уровня для доступа к модулю требуется аутентификация уполномоченного оператора с использованием аутентификационных данных, обеспечиваемых поставщиком.

7.10.7 Руководящие документы

Требования данного пункта гарантируют, что субъекты, использующие криптографический модуль, имеют соответствующее руководство по эксплуатации и процедуры для управления и использования модуля безопасным образом. Руководящими документами могут быть

Руководство администратора и Руководство субъекта, не являющегося администратором.

Руководство администратора - это письменный материал, используемый КС и/или другими субъектами, имеющими роль администратора, для конфигурирования, эксплуатации и управления криптографическим модулем. Руководство администратора содержит информацию и процедуры для управления криптографическим модулем безопасным образом.

В руководстве администратора должны быть определены:

a) административные функции, события безопасности, параметры безопасности (и значения параметров), физические порты, логические интерфейсы криптографического модуля, доступные криптосотруднику и другим субъектам, имеющим роль администратора;

b) процедуры, необходимые для обеспечения функциональной независимости механизмов аутентификации оператора;

c) процедуры для управления криптографическим модулем безопасным образом;

d) допущения, касающиеся поведения пользователя, имеющие отношение к безопасным операциям криптографического модуля.

Руководство субъекта, не являющегося администратором - это письменный материал, используемый пользователем или другими субъектами, не имеющими роль администратора, при эксплуатации криптографического модуля безопасным образом. *Руководство субъекта не являющегося администратором*, включающее инструкции, руководства и предупреждения, описывает функции безопасности криптографического модуля и содержит информацию и процедуры для безопасного использования криптографического модуля.

Руководство субъекта, не являющегося администратором (если реализована роль пользователя) должно определять:

a) утвержденные и не утвержденные функции безопасности, физические порты и логические порты доступные пользователю криптографического модуля;

b) все обязательства пользователя, необходимые для безопасной работы криптографического модуля.

Руководство уполномоченного субъекта с особым личным ключом должно определять:

a) требования к безопасности помещения и оборудования;

b) процедуры, необходимые для генерации и встраивания особого личного ключа в особый аппаратный модуль;

c) регламент.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

7. 11 Подавление прочих атак

В данном стандарте не рассматривается чувствительность криптографического модуля к атакам, которые зависят от типа модуля, реализации и среды работы. Такие атаки могут иметь место относительно криптографических модулей, используемых в среде противника (например, в том случае, когда атакующий может быть авторизованным оператором модуля). Эти атаки зависят от анализа внешней информации. Атаки во всех случаях направлены на определение некоторой информации о КПБ, имеющейся в криптографическом модуле.

Если криптографический модуль спроектирован для подавления одной или нескольких специфических атак, тогда в политике безопасности модуля или других вспомогательных документах должны быть перечислены атаки на модуль, спроектированный для их подавления. Существование и соответствующее функционирование механизмов безопасности, используемых для подавления атак, должны быть обоснованы прежде, чем устанавливаются требования и соответствующие процедуры тестирования.

Дополнительно к требованиям безопасности на первых трех уровнях безопасности к криптографическим модулям на четвертом и пятом уровнях безопасности должно применяться следующее требование:

- если требуется подавление прочих атак, то документация должна определять методы, используемые для подавления атак, и методы тестирования способов подавления.

Приложение А
(обязательное)

Краткие требования к документации

В следующем контрольном перечне представлены требования к документам этого стандарта. Поставщик должен предоставить полный комплект документации для средств, необходимых при проведении тестирования криптографического модуля.

А.1 Спецификации криптографического модуля:

- спецификация элементов аппаратной, аппаратно-программной и программной конфигурации криптографического модуля, спецификация криптографической границы и описание физической конфигурации модуля (первый, второй, третий, четвертый и пятый уровни безопасности);
- спецификация любых элементов аппаратной, аппаратно-программной и программной конфигурации криптографического модуля, к которым не относятся требования безопасности этого стандарта с объяснениями основных причин (первый, второй, третий, четвертый и пятый уровни безопасности);
- спецификация физических портов и логических интерфейсов криптографического модуля (первый, второй, третий, четвертый и пятый уровни безопасности);
- спецификация ручного или логического управления криптографическим модулем, физических или логических индикаторов состояния и соответствующих физических, логических и электрических характеристик (первый, второй, третий, четвертый и пятый уровни безопасности);
- список всех утвержденных в установленном порядке функций безопасности, используемых криптографическим модулем со спецификацией всех режимов работы (первый, второй, третий, четвертый и пятый уровни безопасности);
- блок-схема, изображающая все основные аппаратные компоненты криптографического модуля и компоненты взаимосвязей, включая любые микропроцессоры, буфера ввода-вывода, буфера открытого текста/зашифрованного текста, буфера управления, ключевую память, рабочую память и программную память (первый, второй, третий, четвертый и пятый уровни безопасности);
- спецификация проекта аппаратного и программного обеспечения криптографического модуля (первый, второй, третий, четвертый и пятый уровни безопасности);

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
DEPARTAMENTI

- спецификация всей, связанной с безопасностью, информации, раскрытие или модификация которой может поставить под угрозу безопасность криптографического модуля, например, секретные, особые личные и личные криптографические ключи (в форме открытого и зашифрованного текста), данные аутентификации (пароли, коды), другие КПБ и другая защищаемая информация (события и данные аудита);

- спецификация политики безопасности криптографического модуля, включая правила, установленные требованиями этого стандарта, и правила, полученные из любых дополнительных требований, установленных поставщиком (первый, второй, третий, четвертый и пятый уровни безопасности).

А.2 Физические порты и логические интерфейсы криптографического модуля

Спецификация физических портов и логических интерфейсов криптографического модуля и всех определенных маршрутов ввода и вывода данных (первый, второй, третий, четвертый и пятый уровни безопасности).

А.3 Роли, аутентификация и сервисы:

- спецификация всех уполномоченных ролей, поддерживаемых криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация услуг, операций или утвержденных в установленном порядке функций, обеспечиваемых криптографическим модулем. Для каждой услуги, спецификация сервисного ввода и соответствующий сервисный вывод, а также уполномоченная роль, обеспечиваемая сервисом (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация любых услуг, обеспечиваемых криптографическим модулем, для которых оператор не обязан принимать уполномоченную роль (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация механизмов аутентификации, поддерживаемых криптографическим модулем, типы данных аутентификации, необходимых для поддержания механизмов аутентификации, методы придания полномочий, используемые для управления доступом к модулю при начальной инициализации механизма аутентификации, методы встраивания особого личного ключа в особый аппаратный модуль и стойкость механизмов аутентификации, поддерживаемых модулем, включая обоснование использования поддержки разнообразных механизмов аутентификации (первый, второй, третий, четвертый и пятый уровни безопасности).

А.4 Безопасность программного обеспечения:

- документация должна определять, какие утвержденные в установленном порядке методы целостности используются;
- документация должна определять команды ИПМ, используемые модулем.

А.5 Операционная среда

Спецификация операционной среды криптографического модуля (первый, второй, третий, четвертый и пятый уровни безопасности).

А.6 Физическая защита:

- спецификация аппаратного исполнения и уровень безопасности, который обеспечивается физическими механизмами безопасности криптографического модуля. Спецификация физических механизмов безопасности, которые используются модулем (первый, второй, третий, четвертый и пятый уровни безопасности);
- спецификация интерфейса поддержки доступа и порядок обнуления открытых текстов секретных, личных и особого личного ключей, а также остальных КПБ при обращениях к интерфейсу поддержки доступа, если криптографический модуль поддерживает роль, требующую физического доступа к содержимому модуля, кроме особого личного ключа, или если модуль предназначен для разрешения физического доступа (первый, второй, третий, четвертый и пятый уровни безопасности);
- спецификация нормальных диапазонов функционирования криптографического модуля. Спецификация особенностей защиты от воздействий окружающей среды, используемой криптографическим модулем или спецификация проведения тестирования воздействий окружающей среды (четвертый и пятый уровни безопасности).

А.7 Защита от неразрушающих атак:

- спецификация методов подавления в отношении соответствующих атак ВА (третий, четвертый и пятый уровни безопасности);
- спецификация методов подавления в отношении соответствующих атак УАМ (четвертый и пятый уровни безопасности);
- спецификация методов подавления в отношении соответствующих атак ДАМ (четвертый и пятый уровни безопасности);
- спецификация методов подавления в отношении соответствующих атак ЭМИ (пятый уровень безопасности).

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

А.8 Управление чувствительными параметрами безопасности:

- спецификация всех криптографических ключей, компонентов криптографических ключей и других КПБ, используемых криптографическим модулем;

- спецификация каждого ГСБП, используемого криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация каждого из утвержденных в установленном порядке методов генерации ключей, используемых криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация методов согласования ключей, используемых криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация методов ввода и вывода ключей, используемых криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- доказательство того, что известность *n* ключевых компонентов достаточна для восстановления первоначального ключа, но известность любых *n-1* ключевых компонент не дает никакой информации о первоначальном ключе, кроме длины ключа, если используются процедуры разделения знания (третий, четвертый и пятый уровни безопасности);

- спецификация методов хранения ЧПБ, используемых криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация методов обнуления ЧПБ, в том числе, особого личного ключа, используемых криптографическим модулем (первый, второй, третий, четвертый и пятый уровни безопасности).

А.9 Самотестирование:

- спецификация самотестирования, выполняемого криптографическим модулем, включая предпусковые и условные, и тестирование критичных функций (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация состояний ошибок, вводимых криптографическим модулем, при безуспешном исходе самотестирования, а также состояния и действия, позволяющие выйти из состояния ошибки и возобновить нормальное функционирование модуля (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация всех функций безопасности, важных для безопасного функционирования криптографического модуля и идентификации соответствующего предпускового и обусловленного самотестирования, а также самотестирования критичных функций, выполняемых модулем (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация механизма или логики управления процедурой переключения (для случаев, когда криптографическим модулем производится возможный обход) (первый, второй, третий, четвертый и пятый уровни безопасности).

А.10 Гарантия жизненного цикла:

- спецификация процедур безопасной инсталляции, генерации, встраивания особого личного ключа в особый аппаратный модуль и запуска криптографического модуля (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация процедур для поддержки безопасности в период распределения и поставки версий криптографического модуля уполномоченным оператором (второй, третий, четвертый и пятый уровни безопасности);

- спецификация соответствия между проектом аппаратных средств и программным обеспечением криптографического модуля с его политикой безопасности (то есть правилами операций) (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация исходного текста программного обеспечения, аннотируемого комментариями, которые ясно описывают соответствие программного обеспечения проекту модуля (если криптографический модуль содержит программное обеспечение) (первый, второй, третий, четвертый и пятый уровни безопасности);

- спецификация схемных решений и/или ЯОАО - листинг аппаратных средств (если криптографический модуль содержит аппаратные средства) (первый, второй, третий, четвертый и пятый уровни безопасности);

- функциональная спецификация, которая неформально описывает криптографический модуль, внешние порты и интерфейсы модуля, а также цели интерфейсов (второй, третий, четвертый и пятый уровни безопасности);

- спецификация формальной модели, которая описывает правила и характеристики политики безопасности криптографического модуля с помощью формального языка спецификаций, являющейся нотацией, основанной на строгих положениях математики, типа логики первого порядка или теории множеств (четвертый уровень безопасности);

- спецификация обоснования, которой демонстрирует последовательность и полноту формальной модели относительно политики безопасности криптографического модуля (четвертый уровень безопасности);

- спецификация неформального доказательства соответствия между формальной моделью и функциональной спецификацией (четвертый уровень безопасности);

...STANDART AGENTLIGI
...STANDARTLASHTIRISH,
...MOSLIGINI TEKSHIRISH
VA DAVLAT NAZORATI
...BOSHQARMASI

- для каждого аппаратного и программного компонента должна быть представлена аннотация исходного кода с комментариями, которые определяют (1) предварительные условия, требуемые при входе в компоненту модуля, функцию или процедуру для корректного исполнения и (2) постусловия, ожидаемые в случае успешного завершения использования компоненты модуля и выполнения функции или процедуры (четвертый уровень безопасности);

- спецификация неформального доказательства соответствия между проектом криптографического модуля (как это отражено в аннотациях предварительного условия и постусловия) и функциональной спецификацией (четвертый уровень безопасности);

- спецификация (руководство для криптосотрудника):

a) административные функции, события безопасности, параметры безопасности (и соответствующие их значения), физические порты, а также логические интерфейсы криптографического модуля, доступные криптосотруднику (первый, второй, третий, четвертый и пятый уровни безопасности);

b) процедуры управления криптографическим модулем безопасным способом (первый, второй, третий, четвертый и пятый уровни безопасности);

c) предположения относительно поведения пользователя, которое относится к безопасному функционированию криптографического модуля (первый, второй, третий, четвертый и пятый уровни безопасности);

d) спецификация (руководство для пользователя);

e) утвержденные в установленном порядке функции безопасности, физические порты и логические интерфейсы, доступные пользователям криптографического модуля (первый, второй, третий, четвертый и пятый уровни безопасности); и

f) все обязанности пользователя, необходимые для безопасного функционирования модуля (первый, второй, третий, четвертый и пятый уровни безопасности).

A.11 Подавление прочих атак

Спецификация политики безопасности и механизмов безопасности, используемых криптографическим модулем для подавления атак (если криптографический модуль предназначен для подавления одной или нескольких атак) (первый, второй, третий, четвертый и пятый уровни безопасности).

A.12 Политика безопасности

В соответствии с приложением B (первый, второй, третий, четвертый и пятый уровни безопасности).

Приложение В
(обязательное)

Политика безопасности криптографического модуля

Нижеприведенный перечень резюмирует требования, которые должны быть приведены в политике безопасности. Формат политики безопасности должен быть представлен в порядке, указанном в данном приложении. Политика безопасности не должна быть маркирована как собственная или скопированная без положения, позволяющего копирование или распространение.

Введение

Политика безопасности должна трактовать, в какой степени криптографический модуль соответствует требованиям данного стандарта.

В.1 Спецификация криптографического модуля:

- назначение модуля;
- иллюстративные (пояснительные) схемы, рисунок или фотография модуля. Для аппаратных или особых аппаратных модулей должна быть представлена фотография. Если политика безопасности охватывает различные версии модулей, то каждая версия должна быть представлена отдельно или должно быть упомянуто, что приведены изображения всех версий. Политика безопасности для криптографического модуля в виде программного обеспечения должна содержать блок-схему, которая иллюстрирует:

a) расположение логического объекта программного обеспечения или встроенного программного обеспечения относительно операционной системы, других поддерживаемых приложений и физических границ таким образом, чтобы все логические и физические уровни между логическим объектом и физической границей были четко описаны;

b) взаимодействие между логическим объектом программного обеспечения и встроенным программным обеспечением с операционной системой, а также с другими приложениями, находящимися в пределах физических границ;

- характеристика модуля(ей);
- точная версия/идентификатор модуля и всех компонентов (аппаратного обеспечения, программного обеспечения и встроенного программного обеспечения);
- обозначение программных, гибридных, аппаратных и особых аппаратных модулей;

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

- маркировка программного, гибридного, аппаратного и особо-аппаратного обеспечения;
- перечисление протестированных операционных систем и операционных систем, которые могут быть использованы модулем и которые подтверждены поставщиком (для программных и гибридных модулей) ;
- общие уровни безопасности модуля и уровни безопасности отдельных областей;
- точное определение границ (контуров) модуля;
- утвержденные в установленном порядке режимы работы и инструкции о том, как войти/выйти из какого-либо режима;
- таблица всех функций безопасности с соответствующими длинами ключей, применяемыми в утвержденном в установленном порядке режиме, а также встроенные режимы работы;
- общая стойкость безопасности модуля;
- таблица всех возможных (которые можно вызвать) сервисов;
- блок-схема (при возможности);
- таблица всех ЧПБ, вместе с информацией об их вводе/выводе, генерации, обнулении, и т.д.;
- все документы, касающиеся безопасности и правил работы.

B.2 Порты и интерфейсы криптографического модуля:

- табличный перечень всех портов и интерфейсов (физических и логических);
- определение информации, проходящей через интерфейсы;
- определение физических портов и данных, передаваемых через них.

B.3 Роли, сервисы и аутентификация:

- определение всех ролей;
- таблица ролей с соответствующими сервисами, управляющими вводом и выводом;
- определение каждого метода аутентификации, независимо от того, на чем основан метод: на ролях или на идентичности;
- в какой степени удовлетворяются требования стойкости аутентификации?
- если используется возможность обхода, то какие действия выполняются?
- если используется возможность обхода, то как индицируется статус?
- если загружается внешнее программное обеспечение, определить элементы управления и автономность кода, который определяет несанкционированный доступ и использование модуля;

- описание процесса инсталляции и механизма(ов) криптографической аутентификации;

- если используется особый аппаратный модуль, то описать процесс встраивания особого личного ключа в особый аппаратный модуль.

B.4 Безопасность программного обеспечения:

- установить границы, содержимое и логические механизмы безопасности модуля;

- привести отдельный перечень сервисов безопасности и сервисов, не обеспечивающих безопасность;

- показать каким образом код защищается от подмены?

- показать каким образом увеличена сложность несанкционированного прочтения кода?

- показать, каким образом увеличена сложность несанкционированного прочтения особого личного ключа?

- что такое обнаружение вмешательства и ответные реакции на них?

B.5 Операционная среда:

- указать является ли модуль модифицируемым или нет?

- определить операционную систему и тестируемую платформу;

- разъяснить для каждого уровня, какие требованиям он должен удовлетворять.

B.6 Физическая безопасность:

- определить варианты конструкции (однокристальный, многокристальный встроенный, многокристальный автономный);

- определить варианты встраивания особого личного ключа в особый аппаратный модуль;

- перечислить механизмы физической безопасности, какие требования должны быть удовлетворены для разных вариантов конструкций и уровней безопасности и как оператор может определить, что произошла компрометация.

B.7 Защита от неразрушающих атак:

- для третьего, четвертого и пятого уровней безопасности модулей должно быть описано, каким образом модуль обеспечивает защиту КПБ от атак на основе временного анализа;

- для четвертого и пятого уровней безопасности модулей необходимо указать, обеспечивает ли модуль защиту КПБ, в том числе особого личного ключа от атак УАМ и ДАМ;

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

- для пятого уровня безопасности модулей должно быть описано, каким образом модуль обеспечивает защиту КПБ, в том числе особого личного ключа от атак на основе электромагнитных излучений.

B.8 Управление ЧПБ:

- привести таблицу ключей, определяющую тип(ы) ключа, стойкость в битах, функции безопасности, сертификационный номер функции безопасности, где и как сгенерированы ключи, ключ(и) экспортирован(ы) или импортирован(ы), при использовании метода установки ключа указать любые ключи, имеющие отношение к его установке;
- представить таблицу других КПБ и объяснить, как они сгенерированы;
- детально описать генератор случайных битовых последовательностей (утвержденный в установленном порядке);
- описать использование выходных данных ГСБП;
- детально описать источник(и) энтропии ГСБП;
- детально описать метод(ы) автоматического и ручного ввода/вывода ключей;
- детально описать методы хранения ЧПБ;
- детально описать методы встраивания и хранения особого личного ключа;
- детально описать методы обнуления КПБ и ОПБ и логически обосновать;
- детально описать методы обнуления особого личного ключа и логически обосновать.

B.9 Самотестирование:

- представить перечень предоперационных и условных тестов с определенными параметрами и перечнями условий, на основе которых должны выполняться тесты;
- описать все состояния ошибки с указателями состояния;
- описать запуск операций.

B.10 Гарантия жизненного цикла:

- предоставить описание системы управления конфигурацией и его уникальный идентификатор. Если имеется, то название коммерческой системы;
- описать, как должны выполняться конструкторские требования;
- описать соответствие проекта политике безопасности и МКА (описания могут быть на отдельных документах);
- описать тестирование, выполняемое поставщиком;

- детально описать процедуры доставки и рабочего процесса;
- детально описать требования по сервисам;
- обеспечить криптосотрудника и пользователя руководством (могут быть различные документы);
- обеспечить уполномоченное лицо, реализующее процедуру встраивания особого личного ключа в особый аппаратный модуль, руководством.

B.11 Подавление прочих атак:

- перечислить типы атак, которые могут быть подавлены криптографическим модулем;
- перечислить правила, имеющие отношение к безопасности и ограничения.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHBARMASI

Библиография

[1] FIPS PUB 140-3 (проект), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, U.S. Department of commerce, National Institute of Standards and Technology. Security requirements for cryptographic modules.

[2] ISO/IEC 19790 Information technology – Security techniques – Security requirements for cryptographic modules.

УДК: 621.391 ОКС 35.040 Группа П85

Ключевые слова: аутентификация, атака, безопасность, защита, криптографический модуль, самотестирование, требования, уровень.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Заместитель директора
Центра научно-технических
и маркетинговых исследований _____ Х.П. Хасанов

Главный научный сотрудник
д.т.н., проф. _____ П.Ф. Хасанов

Начальник научно-иесследовательского
отдела криптографии к.т.н. _____ О.П. Ахмедова

Ведущий инженер научно-исследовательского
отдела криптографии _____ Ж.Д. Мукимов

Нормоконтроль _____ Н.К. Травина

СОГЛАСОВАНО

Отдел обеспечения
информационной безопасности
Узбекского агентства связи
и информатизации

Письмо от 01.08.08 № 14-8/2368

СОГЛАСОВАНО

Служба национальной безопасности
Республики Узбекистан

Письмо от 02.09.08 № 39/1152